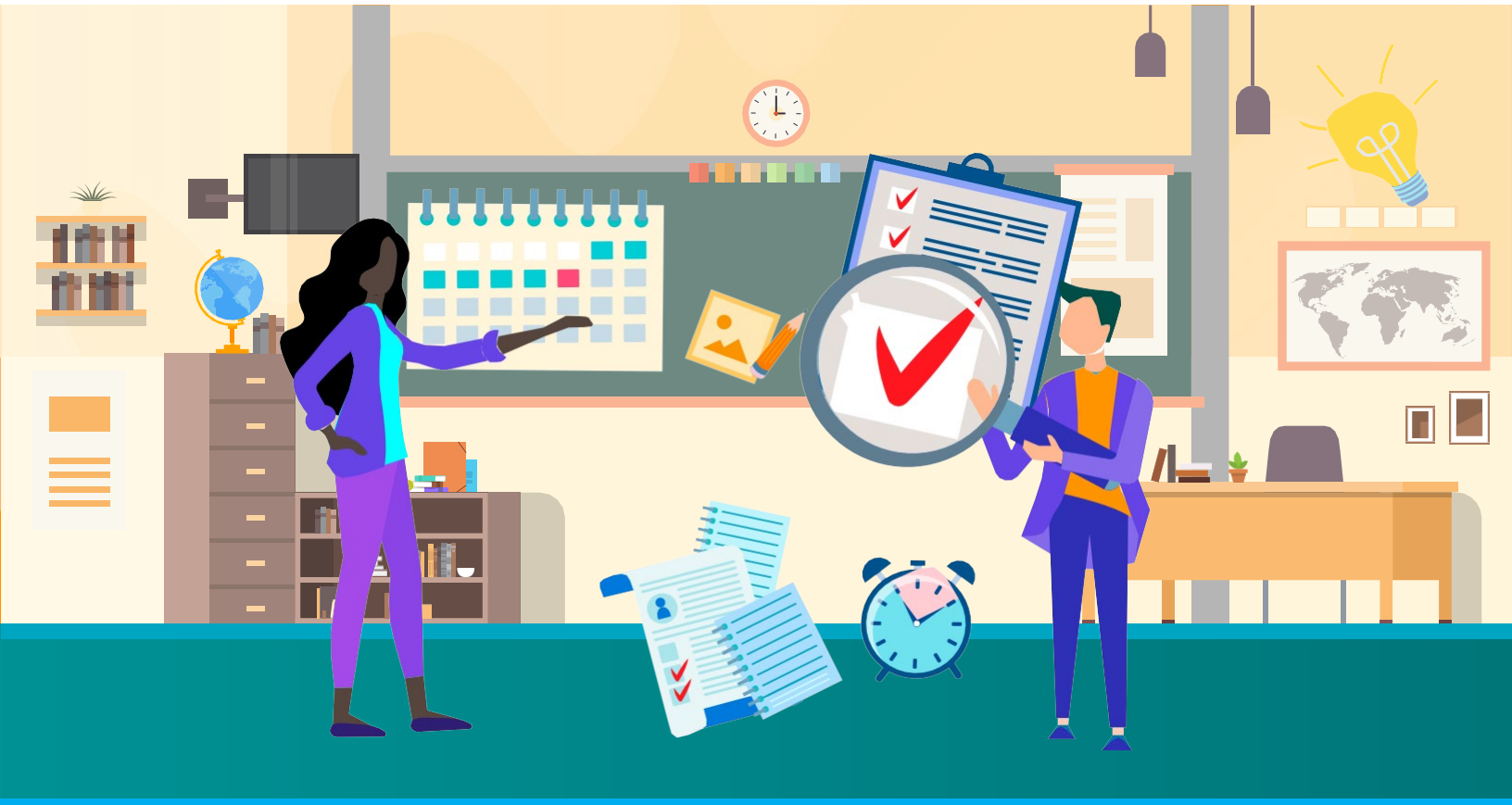
Student Data Privacy and Data Ethics Scenarios for School Leaders



JULY 2023

FUTURE OF PRIVACY FORUM

ABOUT THE FUTURE OF PRIVACY FORUM

The Future of Privacy Forum (FPF) is a nonprofit organization focused on how emerging technologies affect consumer privacy. FPF is based in Washington, DC, and includes an advisory board comprised of leading figures from industry, academia, law, and advocacy groups.

FPF's Youth & Education Privacy program works to protect child and student privacy while allowing for data and technology use that can help young people learn, grow, develop, and succeed. FPF works with stakeholders from practitioners to policymakers, providing technical assistance, resources, trend analysis, and training.

FPF's Youth and Education Privacy team runs Student Privacy Compass, the one-stop-shop resource site on all things related to student privacy.

AUTHORS

Ellen B. Mandinach, PhD *Senior Research Scientist*
WestEd

Jim Siegl
Senior Technologist,
Youth & Education Privacy
Future of Privacy Forum

Jo Beth Jimerson, Ph.D.
Professor, Educational Leadership & Higher Education
Texas Christian University

Melissa Tebbenkamp, MSE, CETL
Technology Leadership and Privacy Consultant
MBBT LLC

ACKNOWLEDGEMENTS

FPF thanks the following individuals for contributing their time, insight, and work in providing feedback on the information in these resources:

Jamie Gorosh
Senior Counsel,
Youth & Education Privacy
Future of Privacy Forum

Bailey Sanchez
Senior Counsel,
Youth & Education Privacy
Future of Privacy Forum

David Sallay
Director,
Youth & Education Privacy
Future of Privacy Forum

Laura Amortegui
Program Manager,
Youth & Education Privacy
Future of Privacy Forum

TABLE OF CONTENTS

Introduction

The Future of Privacy Forum (FPF) has collaborated with Dr. Ellen Mandinach at WestEd and Dr. Jo Beth Jimerson at Texas Christian University to develop resources and teaching scenarios that can be used to help leadership students and current administrators understand issues around data privacy and data ethics, and how these issues intersect with other aspects of school leadership. These materials can be used in educator preparation programs, in in-service training or leadership academies, or as stand-alone materials for self-education. The materials are aligned with many of the standards in the Professional Standards for Educational Leaders (National Policy Board for Educational Administration, 2015) and sections 3 (Education Leaders) and 4 (Coaches) of the ISTE Standards (International Society for Technology in Education, 2018).

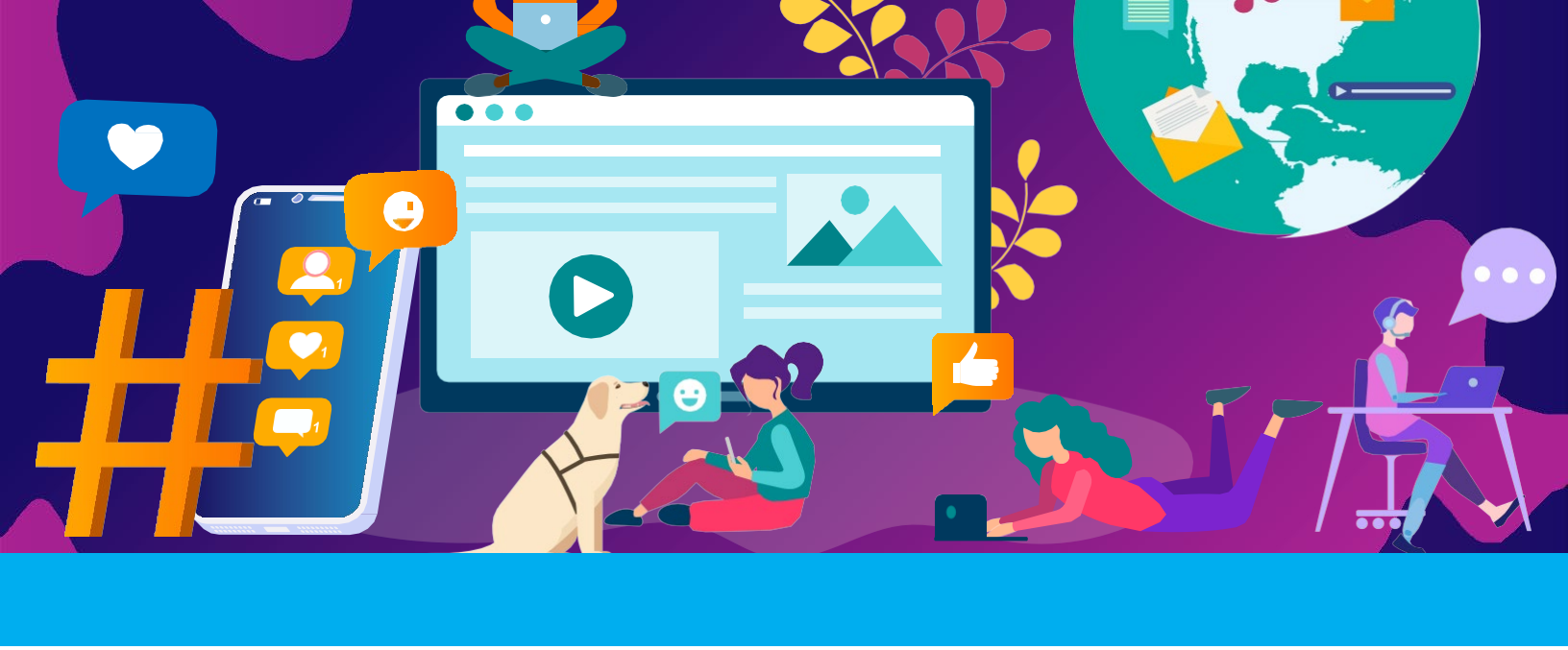
This document serves as a user's guide for resources to help educational leaders better understand data privacy and their role in helping maintain data privacy regulations in their building. Scenarios depict authentic situations that school leaders may encounter in their practice. Many of these situations will likely bubble up from the classroom, where teachers seek assistance from building leadership to guide them in their actions. Other situations may directly focus on leaders. The foundational premise is that building leaders must be aware and knowledgeable about data privacy and help their faculty and staff secure data throughout their schools.

Purpose

Student data privacy and data ethics are essential topics that should be included in educator training and professional development for leaders and teachers. The role of school leaders requires them to make daily decisions that impact which student data is collected or revealed, how the data is stored, how data is interpreted and used to make decisions about students, and how district and state policies are upheld in the classroom. Responsible data use is more than compliance with laws and regulations; it requires practices that ensure ethical and equitable uses of data that work to minimize the potential for harm. The Student Data Privacy and Data Ethics Scenarios for School Leaders are free, supplemental course materials that aim to help educators understand privacy risks and ethical concerns that arise in school-based situations and provide expert guidance on how to mitigate risk and harm through discussions on the legal obligations and best practices for protecting student data privacy.

Audience

These resources were created for the professional development of K-12 school leaders and can be useful at any point in their careers, from leadership candidacy to veteran administrator. Professors of leadership preparation programs can adopt the resources to supplement their course materials. The resources can also be used by professional development providers, technical assistance providers, district in-service staff and administrators, and educators themselves.



How To Use the Resources

These scenarios are meant to be flexible and can be integrated into coursework and professional development training. In educator preparation programs, they can be integrated as assignments, ancillary material, or a complete lesson. They can be used in classes, for small group discussions, and for individual students and can be parts of assignments, essays, lectures, research projects, discussion forums, or other creative projects that instructors may devise. Similarly, in professional development settings, the scenarios can be used for whole or small group discussions or ice breakers.

Facilitators, instructors, professional development providers, and users are free to select the scenarios that they believe to be the most useful and relevant to their learners. Due to the number of scenarios and wide range of topics that target various aspects of student data privacy, we suggest that instructors consider which scenarios or subset of scenarios best fit their particular courses or professional development sessions and learner needs.

Users should feel free to add context and make slight modifications to the scenarios as best meets the needs of their learners. For example, aspiring school leader candidates who have not previously been exposed to school law, and specifically student privacy laws, may require additional background knowledge to critically engage with the scenario and discussion questions. Additionally, facilitators may want to change the grade level or class subject indicated in the scenario to be more relevant to their students. We also provide a Student Privacy Primer for School Leaders that provides a foundation of data ethics and data privacy that can be used for the development of the facilitator and learners.

As the aim of these scenarios is to teach data privacy and data ethics through the discussion of authentic situations, it is critical for the instructor to use framing questions to foster discussion and critical thinking. Learners will get more out of these resources by making connections to their own experiences, learning from others, and spending time in the gray areas posed by the scenarios, as opposed to being told the “right answer”. In addition to the unique discussion questions we include with each scenario, instructors can also use the following overarching and framing questions for the discussion:

- What options does the school leader have in this scenario?
- Why do you think the school leader chose to do that? What do you think was their rationale?
- Is there anything in this situation that is covered under student privacy law or school policy?

Format

Each scenario has a common section for use with both facilitators and learners, and a separate section for facilitators only. The facilitator's version includes all eleven sections, while the student version only includes the first six sections. The learner's version allows facilitators to assign scenarios to their learners, analyze the situation, and answer the discussion questions on their own or in groups without access to guidance.

The scenarios we have developed are meant to be used flexibly. As noted above, they can be used as part of a college or graduate class or supplemental materials. We have drafted each scenario so that a professor or instructor can integrate the materials into the curriculum for class discussion, online interactions, chats, and more. The materials can be used for in-service training. They can also be used for self-study. The scenarios have been developed with the following structure.

Items 1-9 are part of the Learner's section for each scenario.

1. Each scenario begins with a set of **Learning Objectives**. These will help the instructor to integrate the content into existing courses and link the material to professional standards.
2. A **Scenario Narrative** based on an authentic situation that an administrator may face is presented. Some scenarios are short, whereas others may be more complex. The scenario is laid out in a way that the user is confronted with a situation that requires an understanding of data privacy and data ethics. It is written in a way that stimulates consideration on the part of the user of what are the appropriate actions, what might be potential harms, the ramifications of decisions, and more.
3. The scenario narrative is followed by a set of **Discussion Questions**. These questions can be used by instructors in class or through virtual chats to have students discuss some of the fundamental issues encountered in the scenario.

4. The **Evidence Vault** provides research studies that address the situation found in the scenario. These references provide an evidence-based grounding for the situation and the actions administrators may take.
5. A second set of references, **In The News / In the World of Practice**, includes articles that appear in the public media that relate to the scenario. Some scenarios actually draw from the public media, whereas others use articles to show how educators have used data appropriately or less so.
6. The section on **Data Privacy and Compliance Considerations** specifically addresses how these topics play out in the particular scenario.
7. **Ethics/Norms Considerations** moves the discussion past data privacy principles to the role ethics play in the decision-making process.
8. **Leadership Practices and Data Use** describes the role that administrators can or should play in the situation laid out in the scenario. Often, the issues begin at a classroom level, and teachers look to leaders for guidance on handling a situation. It is, therefore, important for leaders to understand the situation and the appropriate actions that should be taken.
9. The final section of the learner material provides additional **References & Resources** that pertain to the particular scenario.

Items 10 and 11 are part of the Facilitator's guide for each scenario.

10. **Teaching Notes** provide the instructors with guidance about how the situation might be addressed in class. The notes highlight nuances around the role of data privacy and data ethics embedded within the scenario.
11. **Extending Activities** allow for a deeper dive into the scenario. It requires the user to consider the ramifications of the scenario. These extended activities can be used in class or for more complex assignments.

Alignment with Professional Standards

The scenarios have been mapped to two sets of professional standards, the Professional Standards for Educational Leaders (PSEL) from the National Policy Board for Educational Administration, and the ISTE Standards for Education Leaders from the International Society for Technology in Education.

SCENARIO	STANDARD
Using Free/Reduced Price Meals Qualification Status to Assign Student Support	**Standards Connections** PSEL • 3(a)-Ensure that each student is treated fairly, respectfully, and with an understanding of each student's culture and context. • 3(b) Recognize, respect, and employ each student's strengths, diversity, and culture as assets for teaching and learning. • 3(e)-Confront and alter institutional biases of student marginalization, deficit-based schooling, and low expectations associated with race, class, culture and language, gender and sexual orientation, and disability or special status. • 3(h)-Address matters of equity and cultural responsiveness in all aspects of leadership. • 9(h)-Know, comply with, and help the school community understand local, state, and federal laws, rights, policies, and regulations so as to promote student success. ISTE Standards • 3.1.d. Cultivate responsible online behavior, including the safe, ethical, and legal use of technology. • 3.3.e. Support educators in using technology to advance learning that meets the diverse learning, cultural, and social-emotional needs of individual students. • 3.4.c. Protect privacy and security by ensuring that students and staff observe effective privacy and data management policies. • 4.6.a. Assist educators and leaders in securely collecting and analyzing student data.
Working with Researchers in Schools	**Standards Connections** PSEL • 2(a)-Act ethically and professionally in personal conduct, relationships with others, decision-making, stewardship of the school's resources, and all aspects of school leadership. • 6(d)-Foster continuous improvement of individual and collective instructional capacity to achieve outcomes envisioned for each student. • 7(g)-Provide opportunities for collaborative examination of practice, collegial feedback, and collective learning. • 7(h)-Encourage faculty-initiated improvement of programs and practices. • 9(h)-Know, comply with, and help the school community understand local, state, and federal laws, rights, policies, and regulations so as to promote student success. ISTE Standards • 3.1.d. Cultivate responsible online behavior, including the safe, ethical and legal use of technology. • 3.4.c. Protect privacy and security by ensuring that students and staff observe effective privacy and data management policies. • 4.6.1. Assist educators and leaders in securely collecting and analyzing student data.

SCENARIO	STANDARD
Student Health Information	**Standards Connections** PSEL • 2(c)-Place children at the center of education and accept responsibility for each student's academic success and well-being. • 5(a)-Build and maintain a safe, caring, and healthy school environment that meets the academic, social, emotional, and physical needs of each student. • 9(b)-Create and sustain positive, collaborative, and productive relationships with families and the community for the benefit of students. • 9(f)-Employ technology to improve the quality and efficiency of operations and management. • 9(h)-Know, comply with, and help the school community understand local, state, and federal laws, rights, policies, and regulations so as to promote student success. • 9(k)-Develop and administer systems for fair and equitable management of conflict among students, faculty and staff, leaders, families, and community. ISTE Standards • 3.4.c. Protect privacy and security by ensuring that students and staff observe effective privacy and data management policies. • 4.6.a. Assist educators and leaders in securely collecting and analyzing student data. • 4.7.b. Partner with educators, leaders, students and families to foster a culture of respectful online interactions and a healthy balance in their use of technology.
Data Sharing with Law Enforcement	**Standards Connections** PSEL • 2(c)-Place children at the center of education and accept responsibility for each student's academic success and well-being. • 2(f)-Provide moral direction for the school and promote ethical and professional behavior among faculty and staff. • 8(b)-Create and sustain positive, collaborative, and productive relationships with families and the community about the school, students, needs, problems, and accomplishments. • 8(j)-Build and sustain productive partnerships with public and private sectors to promote school improvement and student learning. • 9(h)-Know, comply with, and help the school community understand local, state, and federal laws, rights, policies, and regulations so as to promote student success. ISTE Standards • 3.1.d. Cultivate responsible online behavior, including the safe, ethical, and legal use of technology. • 3.4.c. Protect privacy and security by ensuring that students and staff observe effective privacy and data management policies.
Student Surveys	**Standards Connections** PSEL • 5(a)-Build and maintain a safe, caring, and healthy school environment that meets the academic, social, emotional, and physical needs of each student. • 7(e)-Promote and support open, productive, caring, and trusting working relationships among leaders, faculty, and staff to promote professional capacity and the improvement of practice. • 8(b)-Create and sustain positive, collaborative, and productive relationships with families and the community about the school, students, needs, problems, and accomplishments. • 9(h)-Know, comply with, and help the school community understand local,

	state, and federal laws, rights, policies, and regulations so as to promote student success. • 10(g)-Develop technically appropriate systems of data collection, management, analysis, and use, connecting as needed to the district office and external partners for support in planning, implementation, monitoring, feedback, and evaluation. ISTE Standards • 3.1.c. Model digital citizenship by critically evaluating online resources, engaging in civil discourse online and using digital tools to contribute to positive social change. • 3.1.d. Cultivate responsible online behavior, including the safe, ethical, and legal use of technology. • 3.4.c. Protect privacy and security by ensuring that students and staff observe effective privacy and data management policies. • 4.7.b. Partner with educators, leaders, students and families to foster a culture of respectful online interactions and a healthy balance in their use of technology.
Using Video to Increase Learning Opportunities	**Standards Connections** PSEL • 2(e)-Lead with interpersonal and communication skill, social-emotional insight, and understanding of all students' and staff members' backgrounds and cultures. • 3(c) Ensure that each student has equitable access to effective teachers, learning opportunities, academic and social support, and other resources necessary for success. • 4(e)-Promote the effective use of technology in the service of teaching and learning. • 7(g) Provide opportunities for collaborative examination of practice, collegial feedback, and collective learning. • 8(b)-Create and sustain positive, collaborative, and productive relationships with families and the community about the school, students, needs, problems, and accomplishments. ISTE Standards • 3.1.a. Ensure all students have skilled teachers who actively use technology to meet student learning needs. • 3.1.d. Cultivate responsible online behavior, including the safe, ethical, and legal use of technology. • 3.3.d. Support educators in using technology to advance learning that meets the diverse learning, cultural, and social-emotional needs of individual students. • 3.4.c. Protect privacy and security by ensuring that students and staff observe effective privacy and data management policies.

SCENARIO	STANDARD
Using a Personal Device for School Business	**Standards Connections** PSEL • 4(e) Promote the effective use of technology in the service of teaching and learning • 8(b)-Create and sustain positive, collaborative, and productive relationships with families and the community for the benefit of students • 8(c)-Engage in regular and open two-way communication with families and the community about the school, students, needs, problems, and accomplishments • 9(g) Develop and maintain data and communication systems to deliver actionable information for classroom and school improvement • 9(h) Know, comply with, and help the school community understand local, state, and federal laws, rights, policies, and regulations so as to promote student success ISTE Standards • 3.1.d. Cultivate responsible online behavior, including the safe, ethical and legal use of technology. • 3.3.d. Support educators in using technology to advance learning that meets the diverse learning, cultural, and social-emotional needs of individual students. • 3.4.c. Protect privacy and security by ensuring that students and staff observe effective privacy and data management policies. • 4.3.c. Partner with educators to evaluate the efficacy of digital learning content and tools to inform procurement decisions and adoption.
Balancing Parental Pressure and Student Privacy	**Standards Connections** PSEL • 2(b)-Act according to and promote the professional norms of integrity, fairness, transparency, trust, collaboration, perseverance, learning, and continuous improvement. • 2(c)-Place children at the center of education and accept responsibility for each student's academic success and well-being. • 2(e)-Lead with interpersonal and communication skills, social-emotional insight, and understanding of all students' and staff members' backgrounds and cultures. • 8(b)-Create and sustain positive, collaborative, and productive relationships with families and the community for the benefit of students. • 8(c) Engage in regular and open two-way communication with families and the community about the school, students, needs, problems, and accomplishments. ISTE Standards • 3.4.c. Protect privacy and security by ensuring that students and staff observe effective privacy and data management policies. • 4.1.b. Facilitate equitable use of digital learning tools and content that meet the needs of each learner. • 4.1.e. Connect leaders, educators, instructional support, technical support, domain experts and solution providers to maximize the potential of technology for learning

SCENARIO	STANDARD
Data Displays & Data-Driven Celebrations	**Standards Connections** PSEL • 3(b)-Recognize, respect, and employ each student's strengths, diversity, and culture as assets for teaching and learning. • 4(b)-Align and focus systems of curriculum, instruction, and assessment within and across grade levels to promote student academic success, love of learning, the identities and habits of learners, and healthy sense of self. • 4(c)-Promote instructional practice that is consistent with knowledge of child learning and development, pedagogy, and the needs of each student. • 4(g)-Use assessment data appropriately and within technical limitations to monitor student progress and improve instruction. • 5(a)-Build and maintain a safe, caring, and healthy school environment that meets the academic, social, emotional, and physical needs of each student. ISTE Standards • 3.1.d. Cultivate responsible online behavior, including the safe, ethical, and legal use of technology. • 3.4.c. Protect privacy and security by ensuring that students and staff observe effective privacy and data management policies. • 4.6.c. Partner with educators to empower students to use learning data to
Online Activity & Threat Monitoring	**Standards Connections** PSEL • 3(d) Develop student policies and address student misconduct in a positive, fair, and unbiased manner. • 3(e)-Confront and alter institutional biases of student marginalization, deficit-based schooling, and low expectations associated with race, class, culture and language, gender and sexual orientation, and disability or special status. • 3(f)-Promote the preparation of students to live productively in and contribute to the diverse cultural contexts of a global society. • 5(a)-Build and maintain a safe, caring, and healthy school environment that meets the academic, social, emotional, and physical needs of each student. • 5(b)-Create and sustain a school environment in which each student is known, accepted and valued, trusted and respected, cared for, and encouraged to be an active and responsible member of the school community. • 8(b)-Create and sustain positive, collaborative, and productive relationships with families and the community about the school, students, needs, problems, and accomplishments. • 9(h)-Know, comply with, and help the school community understand local, state, and federal laws, rights, policies, and regulations so as to promote student success. ISTE Standards • 3.1.d. Cultivate responsible online behavior, including the safe, ethical, and legal use of technology. • 3.4.c. Protect privacy and security by ensuring that students and staff observe effective privacy and data management policies. • 4.7.b. Partner with educators, leaders, students and families to foster a culture of respectful online interactions and a healthy balance in their use of technology.

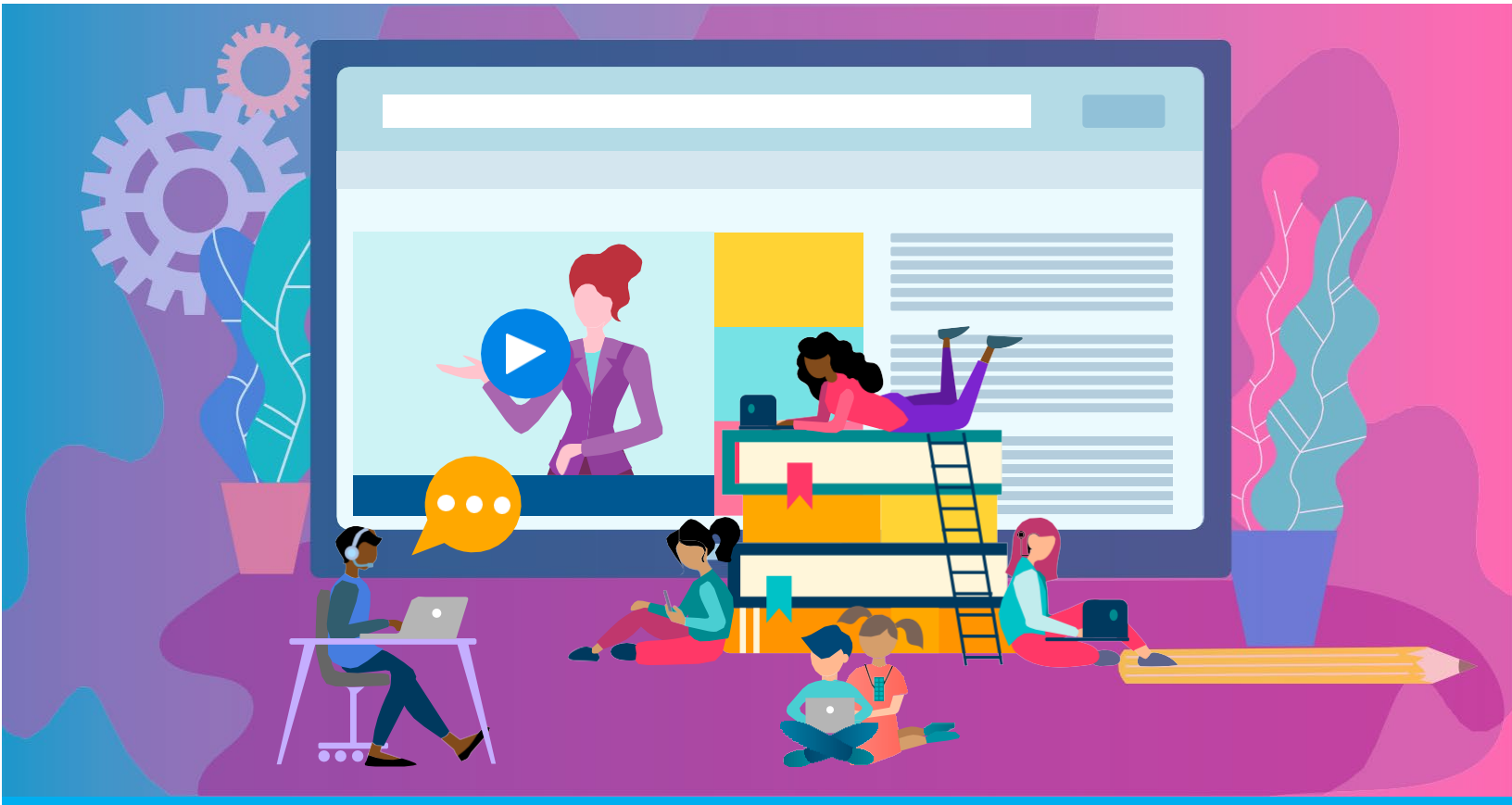
SCENARIO	STANDARD
Data Dashboards & Early Warning Systems	**Standards Connections** PSEL • 4(e) Promote the effective use of technology in the service of teaching and learning • 8(b)-Create and sustain positive, collaborative, and productive relationships with families and the community for the benefit of students • 8(c)-Engage in regular and open two-way communication with families and the community about the school, students, needs, problems, and accomplishments • 9(g) Develop and maintain data and communication systems to deliver actionable information for classroom and school improvement • 9(h) Know, comply with, and help the school community understand local, state, and federal laws, rights, policies, and regulations so as to promote student success ISTE Standards • 3.1.d. Cultivate responsible online behavior, including the safe, ethical and legal use of technology. • 3.3.d. Support educators in using technology to advance learning that meets the diverse learning, cultural, and social-emotional needs of individual students. • 3.4.c. Protect privacy and security by ensuring that students and staff observe effective privacy and data management policies. • 4.3.c. Partner with educators to evaluate the efficacy of digital learning content and tools to inform procurement decisions and adoption.
De-Identified and Aggregate Student Data	**Standards Connections** PSEL • 3(d) Develop student policies and address student misconduct in a positive, fair, and unbiased manner. • 3(e)-Confront and alter institutional biases of student marginalization, deficit-based schooling, and low expectations associated with race, class, culture and language, gender and sexual orientation, and disability or special status. • 3(f)-Promote the preparation of students to live productively in and contribute to the diverse cultural contexts of a global society. • 5(a)-Build and maintain a safe, caring, and healthy school environment that meets the academic, social, emotional, and physical needs of each student. • 5(b)-Create and sustain a school environment in which each student is known, accepted and valued, trusted and respected, cared for, and encouraged to be an active and responsible member of the school community. • 8(b)-Create and sustain positive, collaborative, and productive relationships with families and the community about the school, students, needs, problems, and accomplishments. • 9(h)-Know, comply with, and help the school community understand local, state, and federal laws, rights, policies, and regulations so as to promote student success. ISTE Standards • 3.1.d. Cultivate responsible online behavior, including the safe, ethical, and legal use of technology. • 3.4.c. Protect privacy and security by ensuring that students and staff observe effective privacy and data management policies. • 4.7.b. Partner with educators, leaders, students and families to foster a culture of respectful online interactions and a healthy balance in their use of technology.

SCENARIO	STANDARD
Cyberbullying & Social Media	**Standards Connections** <u>PSEL</u> • 1(c)-Articulate, advocate, and cultivate core values that define the school's culture and stress the imperative of child-centered education; high expectations and student support; equity, inclusiveness, and social justice openness, caring, and trust; and continuous improvement. • 2(c)-Place children at the center of education and accept responsibility for each student's academic success and well-being. • 2(d)-Safeguard and promote the values of democracy, individual freedom and responsibility, equity, social justice, community, and diversity. • 3(a)-Ensure that each student is treated fairly, respectfully, and with an understanding of each student's culture and context. • 3(d) Develop student policies and address student misconduct in a positive, fair, and unbiased manner. • 3(e)-Confront and alter institutional biases of student marginalization, deficit-based schooling, and low expectations associated with race, class, culture and language, gender and sexual orientation, and disability or special status. • 3(f)-Promote the preparation of students to live productively in and contribute to the diverse cultural contexts of a global society. • 3(h)-Address matters of equity and cultural responsiveness in all aspects of leadership. • 4(e)-Promote the effective use of technology in the service of teaching and learning. • 5(a)-Build and maintain a safe, caring, and healthy school environment that meets the academic, social, emotional, and physical needs of each student. • 5(b)-Create and sustain a school environment in which each student is known, accepted and valued, trusted and respected, cared for, and encouraged to be an active and responsible member of the school community. • 5(d)-Promote adult-student, student-peer, and school-community relationships that value and support academic learning and positive social and emotional development. • 8(b)-Create and sustain positive, collaborative, and productive relationships with families and the community about the school, students, needs, problems, and accomplishments. • 9(h)-Know, comply with, and help the school community understand local, state, and federal laws, rights, policies, and regulations so as to promote student success. <u>ISTE Standards</u> • 3.1.c. Model digital citizenship by critically evaluating online resources, engaging in civil discourse online and using digital tools to contribute to positive social change. • 3.1.d. Cultivate responsible online behavior, including the safe, ethical, and legal use of technology. • 3.3.e. Support educators in using technology to advance learning that meets the diverse learning, cultural, and social-emotional needs of individual students. • 3.4.c. Protect privacy and security by ensuring that students and staff observe effective privacy and data management policies. • 4.7.b. Partner with educators, leaders, students and families to foster a culture of respectful online interactions and a healthy balance in their use of technology. • 4.7.d. Empower educators, leaders and students to make informed decisions to protect their personal data and curate the digital profile they intend to reflect.

SCENARIO	STANDARD
Balancing Student Privacy and Academic Integrity	**Standards Connections** PSEL • 3(a)-Ensure that each student is treated fairly, respectfully, and with an understanding of each student's culture and context. • 3(d)-Develop student policies and address student misconduct in a positive, fair, and unbiased manner. • 3(h)-Address matters of equity and cultural responsiveness in all aspects of leadership. • 4(e)-Promote the effective use of technology in the service of teaching and learning. • 6(d)-Foster continuous improvement of individual and collective instructional capacity to achieve outcomes envisioned for each student. • 10(g)-Develop technically appropriate systems of data collection, management, analysis, and use, connecting as needed to the district office and external partners for support in planning, implementation, monitoring, feedback, and evaluation. ISTE Standards • 3.1.c. Model digital citizenship by critically evaluating online resources, engaging in civil discourse online and using digital tools to contribute to positive social change. • 3.1.d. Cultivate responsible online behavior, including the safe, ethical, and legal use of technology. • 3.3.e. Support educators in using technology to advance learning that meets the diverse learning, cultural, and social-emotional needs of individual students. • 3.4.c. Protect privacy and security by ensuring that students and staff observe effective privacy and data management policies.
A Basic App Vetting/Approval Scenario	**Standards Connections** PSEL • 3(a)-Ensure that each student is treated fairly, respectfully, and with an understanding of each student's culture and context. • 3(d)-Develop student policies and address student misconduct in a positive, fair, and unbiased manner. • 3(h)-Address matters of equity and cultural responsiveness in all aspects of leadership. • 4(e)-Promote the effective use of technology in the service of teaching and learning. • 6(d)-Foster continuous improvement of individual and collective instructional capacity to achieve outcomes envisioned for each student. • 10(g)-Develop technically appropriate systems of data collection, management, analysis, and use, connecting as needed to the district office and external partners for support in planning, implementation, monitoring, feedback, and evaluation. ISTE Standards • 3.1.c. Model digital citizenship by critically evaluating online resources, engaging in civil discourse online and using digital tools to contribute to positive social change. • 3.1.d. Cultivate responsible online behavior, including the safe, ethical, and legal use of technology. • 3.3.e. Support educators in using technology to advance learning that meets the diverse learning, cultural, and social-emotional needs of individual students. • 3.4.c. Protect privacy and security by ensuring that students and staff observe effective privacy and data management policies.

References

- Anderson, S., Leithwood, K., & Strauss, T. (2010). Leading data use in schools: Organizational conditions and practices at the school and district levels. *Leadership and Policy in Schools, 9*(3), 292-327. https://doi.org/10.1080/15700761003731492
- Booher-Jennings, J. (2005). Below the bubble: "Educational triage" and the Texas accountability system. *American Educational Research Journal, 42*(2), 231-268.
- Daly, A. J. (2009). Rigid response in an age of accountability. *Educational Administration Quarterly, 45*(2), 168-216. 10.1177/0013161X08330499
- Datnow, A., (2017). *Opening or closing doors for students? Equity and data-driven decision-making*. Retrieved from https://research.acer.edu.au/cgi/viewcontent.cgi?article=1317&context=research_conference
- Datnow, A., Greene, J. C., & Gannon-Slater, N. (2017). Data use for equity: Implications for teaching, leadership, and policy. *Journal of Educational Administration, 55*(4), 3544-360. https://doi.org/10.1108/JEA-04-2017-0040
- Datnow, A., & Park, V. (2018). Opening or closing doors for students? Equity and data use in schools. *Journal of Educational Change*, *19*(2), 131-152.
- ISTE. (n.d.). *ISTE standards*. https://cdn.iste.org/www-root/ISTE%20Standards-One-Sheet_Combined_11-22-2021_vF4%20(1)%20(4).pdf
- Jimerson, J.B., Garry, V., Poortman, C. L., & Schildkamp, K. (2021). Implementation of a collaborative data use model in a United States context. *Studies in Educational Evaluation, 69,* 100866. https://doi.org/10.1016/j.stueduc.2020.100866
- Mandinach, E. B., & Gummer. (Eds.). (2021). *The ethical use of data in education: Promoting responsible policies and practices*. Teachers College Press.
- Marsh, J.A., Farrell, C.C., & Bertrand, M. (2016). Trickle-down accountability: How middle school teachers engage students in data use. *Educational Policy, 30*(2), 243-280. DOI: 10.1177/0895904814531653
- National Policy Board for Educational Administrators. (2015). *Professional standards for educational administrators.* https://www.npbea.org/wp-content/uploads/2017/06/Professional-Standards-for-Educational-Leaders_2015.pdf
- Schildkamp, K. (2019). Data-based decision-making for school improvement: Research insights and gaps. *Educational Research, 61* (3), 257-273. https://doi.org/10.1080/00131881.2019.1625716



STUDENT DATA PRIVACY AND DATA ETHICS SCENARIOS FOR SCHOOL LEADERS

Using a Personal Device for School Business

Learning Objectives

- Describe the differences in FERPA-compliant collaboration around student needs and unnecessary sharing/distribution of personally identifiable information (PII).
- Identify information that is shareable via approved, vetted technology devices and apps versus data and information collected via personal devices and/or unapproved apps.
- Identify the risks associated (to students and employees) with using personal devices and/or unvetted apps in ways that capture and report PII about students.
- Delineate laws that apply to apps designed for student use, apps designed for teacher/educator use, and how district-level IT processes can mitigate the risk of loss of data privacy or other harms.

Dr. Tasha Cho, principal of Creekside Elementary School, received a subpoena pertaining to a fourth-grade student, Dylan Little, as a part of a divorce and custody proceeding. The subpoena requested all "school records and communications" for the last two years and specified "any records pertaining to Dylan Little found on the cell phones or personal computers of administrators or teachers" and included "educational records maintained in any and all data or communications systems."

Dr. Cho, Mr. Erwin, the school's attorney, and the IT department worked to pull the requested records from all district data systems, including the student information system, learning management system, email, internal messaging program, and managed instructional software. Dr. Cho also made copies of Dylan's physical school records. Mr. Erwin directs Dr. Cho to determine if any staff member had communications or other educational records on personal devices.

Dr. Cho discovered that the Assistant Principal had text message correspondence with Dylan's dad on his personal cell phone. In addition, his current teacher had used her personal phone at school to text Dylan's mom about his Accelerated Reader progress. She also uses her personal phone to update the "Super Student Check-In" app, which provides real-time communication about student academic and behavioral goals. This is not a standard district application; it only runs on iOS or Android, so it is not accessible from the district computer and is voluntary for parents to use for parent-teacher communication. However, all students are tracked in the app.

Upon review of the email communication pulled, Mr. Erwin noted math progress in several applications reported to Mom. However, those applications were not part of the district-managed data provided by IT. After a discussion with Dr. Cho, it was determined that the apps were online programs used by Dylan's third-grade teacher, who was no longer with the district.

Discussion Questions

- What should Dr. Cho do in response to the subpoena? Are there any actions she should take beyond dealing with the current situation in terms of communication between staff and parents? If so, what?
- How do challenges, and risks, regarding educational records and the parent's rights to access vary depending on if the data and/or application is managed by the district?
- Are the text messages on the AP's and teacher's phones education records subject to disclosure, since they are stored on personal devices and the school can only control/search their own technology and files?
- Should the teacher or AP delete their text messages? Why or why not? Would deleting messages (related to Dylan or to other students) solve the problem or make the situation worse? Explain.
- What norms should Dr. Cho work to establish, or what practices should she initiate, to help prevent such issues from happening again, while still encouraging regular, open, and honest communication with parents?
- Given the ease of using personal devices and online applications, how could leaders set expectations for data privacy, particularly related to school business and/or students, to minimize risk? What policies or procedures might need to be implemented to ensure data privacy is maintained in compliance with FERPA?
- What policies/procedures do you have around the use of personal devices, parent communication, and data systems? How might your current policies and procedures assist you if you were to receive a similar subpoena? What changes might be needed?

From the Evidence Vault:

- Barnes, K. (2015). The challenge of data privacy. Educational Leadership 73(3), 40-44.
- Congressional Research Service (2021, May 24). The Family Educational Rights and Privacy Act (FERPA): Legal issues. R46799 https://files.eric.ed.gov/fulltext/ED614263.pdf
- Hitch, R., & McPherson, B. (2018). But it's my cell phone: Methods and consequences of using a personal device for school business. Schwartz & Shaw, Raleigh, NC. Presented at the 2018 School Law Seminar, San Antonio, TX. https://cdn-files.nsba.org/s3fs-public/02_07_But_It's_My_Cell_Phone_Hitch_McPherson.pdf
- Kumar, P. C., Chetty, M., Clegg, T. L., & Vitak, J. (2019, May). Privacy and security considerations for digital technology use in elementary schools. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (pp. 1-13). https://dl.acm.org/doi/pdf/10.1145/3290605.3300537
- Underwood, J. (2017). Under the law: You say 'records,' and I say 'data'. Phi Delta Kappan 98(8), 74-75.

In the News / In the World of Practice:

- EdTech Review Editorial Team (2022, April 8). How teachers can text families–without their personal phones. EdTech Review. https://edtechreview.in/trends-insights/trends/5641-how-teachers-can-text-families-without-their-personal-phones
- Lungwitz, K. (2022). Your 'private' texts may be public information: An update on the Public Information Act and The Open Meetings Act. Texas Elementary Principals and Supervisors Association. https://www.tepsa.org/resource/your-private-texts-may-be-public-information-an-update-on-the-public-information-act-and-the-open-meetings-act/
- Singer, N. (2014, November 16). Privacy concerns for ClassDojo and other tracking apps for schoolchildren. The New York Times. https://www.nytimes.com/2014/11/17/technology/privacy-concerns-for-classdojo-and-other-tracking-apps-for-schoolchildren.html

Data Privacy and Compliance Considerations

There are several intersecting issues related to data privacy and devices here, and as laws evolve, it will be important for school leaders to ensure that they stay abreast of developments in education law through their respective school district attorneys.

One issue related to data privacy involves data stored in the "Super Student Check-In" app (an app fictionalized for the purposes of this learning scenario). If the app has been appropriately vetted by and approved for use by the district, release of data from the app (whether accessed via a personal phone, a school-owned device or computer) should not be complicated. In fact, the district IT department ought to be able to pull any communications or data related to Dylan to comply with the subpoena. This can be a benefit of third-party communication apps vetted for compliance by school districts, and paid for by school districts: If security measures meet standards, and the data are stored not on individual devices, or personal service but in a secured server or cloud, then district IT can search and pull data for compliance purposes as they would data from a student information system or any district-owned system. The release of data collected, stored, and disseminated via the app (including any messaging function used within the app) may not be as complicated if the district has approved use and the data pertinent to the student can be pulled from district systems.

The situation may be more complicated if the employees have tried to circumvent district policies and approval processes, and have signed up on their own for use of an app. In that case, the app may not be properly vetted for security, which could put any student data (even names and contact information) at risk of unauthorized disclosure. This is why approval processes and data agreements are critical when districts use free or purchased software that will manage student information, including communications with parents.

In this case, communications could only be accessed via the employee's device or account.

If employees are using the standard texting functions of their devices (tablets, phones), they may be creating a record by including student names and PII (grades, absences, discipline infractions).

Though in the past, some courts have held that a "student record" is only that physically stored in a school file (physically or electronically), technology and the law regarding the intersection of student records and digital communication continues to evolve (Francek P.C., 2013). Given this evolution, it's difficult to imagine that written texts, or photos captured via personal devices that can identify children, would be exempt from subpoenas for "any and all communications" relating to a student. After all, emails discussing particular students are already subject to subpoenas and records requests, even when they are not physically printed out and placed in student cumulative files.

In custody cases in particular, attorneys may seek to establish patterns of communication with the school, so teachers and other personnel might be wise to communicate only from school-owned devices, from email or texting services/apps dedicated to professional work, and through district-owned apps that route communication though non-personal channels (even if the employee accesses the app via a personal device). State laws in Texas require school employees to preserve public information stored on personal devices. The Washington Supreme Court unanimously held in Nissen v. Pierce County that text messages sent or received by a public employee in his or her official capacity are public records within the meaning of the Public Records Act (PRA), even if the employee is using a personal cell phone.

Ethics and Norms

Though this subpoena seemed worded as a "catch-all" (and it's not clear a judge would approve something so broad), the individual educators in this scenario would be wise to talk with legal representation or union representation, as appropriate, in navigating any potential searches of their personal devices. The district is not an arm of law enforcement, and could not compel the teachers and administrators to permit the district to perform a search of employees' personal devices. Personal employee devices should not be subject to search by employers. (if there is a valid reason a district needs to know what is in an employee's personal device, they may also seek legal means to do so.) In this scenario, the employees could choose to comply, but a cleaner solution would be for the court to subpoena school-based document/communication from the district, and to seek separate subpoenas for the personal devices of individuals.

Regardless of whether the subpoena at hand names the teachers/administrators as individuals and specifies their personal devices (as this subpoena seemed aimed at the school/school communication systems itself), it would be unwise for the educators to try to delete information from their personal devices after receiving the subpoena, even if they themselves are not the identified target/recipient of the subpoena, as it's possible that a court could determine such action to be out of line given the "notice" that a party to legal action is seeking the information. School and district leaders should not be demanding that employees turn over personal devices for search in their role as campus/district leaders, lest they run afoul of illegal search and seizure prohibitions.

Sometimes, communications by adult employees via text message or other social media with students is prohibited by law or ethics codes. Communicating with parents or legal guardians via text is not prohibited, though doing so from a personal device and from a personal phone number or email lowers boundaries that can protect educators and create complications. Communicating about students, and/or communicating about student data via a personal device

can open a window for legal requests related to students on personal devices. Integrated phone systems can allow educators to route texts and phone calls through computer software to maximize the opportunity to use district-owned technology for communications. If educators limit communication about specific students to school-owned technology, or via school-owned/provided and supported communication apps they can at least have a measure of system security as to the storage of such data while maintaining a measure of privacy and home/work boundaries for educators.

In this scenario, it appears that Ms. Flowers and Mr. Halpern were both trying to be supportive and to foster positive relationships with parents to benefit Dylan. At the same time, the ways in which they communicated may set up a situation where each employee is deposed or testifying on behalf of opposing parties in the legal matter pending. Providing useful information, via appropriate devices, and in ways that do not deride either parent is important if the goal is supporting the student. Educators should always communicate with a parent or guardian assuming that other persons with custodial rights (and a court) could eventually view the communication. Calm, factual communication is important, as is choosing what venues to use for that communication. Handled poorly, trust between the parents and school could be harmed if educators start to share derogatory communication about one parent/guardian with another.

Leadership Practices & Data Use

This could be a fairly simple or complicated situation, depending on several of the variables outlined in the previous section. In any case, Dr. Cho needs to communicate clearly with the school district's attorney and her own supervisor. It may be the case that, while the texts may be subject to subpoena, the court must subpoena them separately from the school. What is clear is that using personal devices to communicate with parents about private information related to a specific child has now contributed to a complicated situation for the school and some school employees to navigate.

It's admirable that the AP and teacher want to engage with the parents regularly and in ways that meet the parents' needs. Still, educators need to keep in mind that any communication with parents (or others) about students is likely to be subject to disclosure requests by parents or legal guardians (except in "sole possession" or some cases with counseling services). What might seem friendly in a text message to one parent might take on a whole new context when published or presented in a court proceeding. A good guide is for educators to never write something to one parent that they would not mind other parents/legal guardians reading.

School leaders often (and appropriately) encourage frequent communication with parents/guardians, but leaders also need to ensure that they are providing educators with appropriate guidelines and protections for communicating in ways that are productive and protect data privacy (Park et al., 2021). This means providing guidelines for content (e.g., only sharing information that, if viewed by other parties, would be considered professional and appropriate to educational goals), and guidelines that outline what persons are eligible to receive such communication (e.g., ensuring that persons requesting communication are legally entitled to that communication, and abiding by any custodial restrictions on file with the school). It may also mean working with district IT personnel to determine the appropriateness or availability of third-

party communication apps that can house educator-parent/guardian communications without requiring teachers or other personnel to use personal cell phone numbers or to engage in direct texting or other communications. Finally, leaders need to be cognizant of how communication preferences and habits can shift with generational preferences–they may need to tailor guidance to the ways in which various employees at different life stages feel comfortable communicating in the private lives, and highlight how communication in the professional sphere requires adjusted practices due to raised stakes and protections (Janssen & Carradini, 2021).

Finally, school leaders who encourage the use of apps for communication should do due diligence to ensure that app use does not place an undue burden on families in terms of financial costs or in terms of having to agree to data sharing in order to send or receive communication via the app. In some cases, apps may be free to the school, but require parents/guardians to pay a fee or agree to particular data sharing to make full use of the app. If the app has been vetted by the district, schools should be able to work out agreements that do not require families to pay fees or share data in excess of what the school has agreed to in their vetting/data sharing or storage process. Without those protections, some families will have more access to the app's benefits/communication than others, and families may feel pressured to agree to data sharing provisions (e.g., for marketing purposes) to which they would otherwise not agree. Without attention to what is being used, and what burdens use places on both school personnel and students' families, well-intended educators could be contributing to equity issues (see Future of Privacy Forum, 2021)

References and Resources

- Complying with COPPA: Frequently Asked Questions (2020, July). Federal Trade Commission. Retrieved from https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions
- Franczek P.C. (2013, February 20). Are emails, texts, tweets, and other digital communications student records under FERPA and state law? JDSUPRA. https://www.jdsupra.com/legalnews/are-emails-texts-tweets-and-other-dig-60950/
- Janssen, D. & Carradini, S. (2021). Generation Z workplace communication habits and expectations. IIEE Transactions on Professional Communication 64(2), 137-153. https://ieeexplore.ieee.org/document/9440009
- Jones, S. (2020). Texting relationships between students and staff. AASA School Administrator. https://my.aasa.org/AASA/Resources/SAMag/2020/Apr20/Legal.aspx
- Park, J., Cotto, J., Waller Curtis, A., Klein, C. Reddy, A., Siegl, J, Sollberger, A., Triplett, J. & Vance, A. (2021, January 12). Student privacy communications toolkit: For schools & districts. Future of Privacy Forum. https://studentprivacycompass.org/resource/student-privacy-communications-toolkit-for-schools-districts/
- Future of Privacy Forum (2021, October 5) Student privacy primer. https://studentprivacycompass.org/resource/student-privacy-primer/
- Law requires school employees to preserve public information stored on personal devices https://www.tcta.org/latest-education-news/law-requires-school-employees-to-preserve-

public-information-stored-on-personal-devices

- But It's My Cell Phone: Methods and Consequences of Using a Personal Device for School Business, https://cdn-files.nsba.org/s3fs-public/02_07_But_It's_My_Cell_Phone_Hitch_McPherson.pdf Rachel Hitch, Brandon McPherson Council of School Attorneys
- Sommaruga, M., Student E-Mails, FERPA and FOIA: What School Districts Must Disclose (and When)? https://www.pullcom.com/education-law-notes/student-e-mails-ferpa-and-foia-what-school-districts-must-disclose-and-when

Facilitator's Guide: Using a Personal Device for School Business

Teaching Notes and Considerations for Scenario Facilitators:

In this scenario, users will encounter one form of challenge in school-family communication: the tension between wanting to be welcoming and supportive of parents while also keeping in mind that communications that identify students and contain other PII are inevitably available to the student's custodians. Of course, there are other dangers related to text messaging–highlighted in the media when educators unethically (and sometimes illegally) engage in inappropriate communications with students (Jones, 2020). This scenario focuses not on those obvious breaches of law and ethics, but on what may happen if even well-intended educators are not circumspect about what they put in print (in text messages) with family members or even other educators, and how this can be complicated if communications ensue from personal devices and/or from unauthorized apps.

Extending Activities

- Look up the policies that exist in your district/organization regarding the use of personally-owned devices. What restrictions, if any, exist? What other forms of security (e.g., two factor authentication) help protect data accessed in the event a device (personally or district-owned) is lost, stolen, or otherwise compromised?
- If you have access to an attorney who works for the district, ask the attorney what they would advise an employee who finds themselves in the situation posed in this case. What do they suggest educators in your district/organization do to communicate well and efficiently with families and students, but to also protect themselves from putting their own data and communications at risk?

Online Activity & Threat Monitoring

Learning Objectives

- Explain when and under what conditions schools have legal and/or ethical duties to address inappropriate student behavior when using technology.
- Discuss how the goals of protecting student privacy and safeguarding students can conflict with or complement one another.
- Delineate actions that can be taken by teachers, leaders, and technology specialists to mitigate risk to students or otherwise help students develop the knowledge, behaviors, and skills needed to protect themselves with regard to technology, communication apps, and social media use.
- Explain pathways to disciplinary, counseling, or other administrative action and the potential barriers to such actions as they relate to inappropriate online behavior depending on whether the conduct occurs on or off campus, during or outside of school hours, and on school-owned or personal technology devices (including networks).
- Identify when it is appropriate to involve local police, and what information can be shared, as a result of alerts from online activity and threat monitoring systems.

Dunkin School District is considering adding tools to its current content filter. These tools include monitoring for and reporting on the following activity: (1) email alerts for inappropriate keyword searches, (2) email and/or text alerts for dangerous or self-harm searches, (3) email and/or text alerts for student self-harm or threat activity on any online platform including online documents, social media and communication apps, and (4) monitoring/alert service by the vendor which can include notification of local police.

A committee has been formed to evaluate the ethical and legal considerations of each tool and how the district should balance student safety and privacy. As part of the committee review process, they are presented with possible alerts that may arise from using the tools. They debate how they should respond to each alert in an effort to develop policies and internal procedures around the use of the tools. Before the discussion, they are reminded that in addition to student activity on district devices, the tools may monitor students when they are logged into the browser with the district account or authenticated to a site/app with their district account, even if they are using a personal or non-district device. The committee reviews the following scenarios:

- A seventh-grade student's social media post has triggered an alert for potential bullying. The post by Clay contains a picture of Sam and Clay at a school-related event. Several other students have commented on the photo, and some comments are mean and derogatory. One comment suggests that Sam should kill themselves and another threatens to assault Clay. The post and all comments occurred after school hours. Since social media is blocked on district devices, the alert originated from activity on a non-district device.
- A student at the elementary school has created a collaborative online document and shared it with all students in the class, but not the teacher. The students use this document

as a “hidden chat room.” The document triggers a potential bullying alert as two students use the comment feature to call other students derogatory names and threaten to remove them from the document.

- A potential self-harm alert is triggered on Susie’s search history as she has multiple searches on signs of depression, methods of suicide, and different types of kitchen knife blades. The counselor knows that the health class is doing a unit on mental health and sees that Susie is enrolled in a health and cooking class.
- An inappropriate search alert is triggered for three middle school students who have used several search terms that appear to be sexual in nature as well as inappropriate language. Some of the search terms are similar to popular lyrics.
- The vendor threat monitoring service has identified a student who may be a high suicide risk. The alert came in after hours and the student is off campus. The student is known by the school leadership team as a youth who is being treated for mental health concerns. The service offers to contact the local police for a wellness check and asks how to proceed and what information should be shared.
- A potential threat alert is triggered by a student’s after-hours search for the following terms: bomb, guns, school shooting, assault rifle, school fire drills, and how to start a big fire. The alert is received after hours through text and email to all designated building leadership. The student has recently been disciplined for outbursts in the classroom and is serving a three-day out-of-school suspension.

Discussion Questions

- Assess how each alert may be approached. Should students or parents be approached? If so, by who?
    - What risks attach to the decision, and what policies or ethics guides are needed around what should (or needs to) be shared, with whom, and when?
    - What additional actions/investigations may occur before deciding how to proceed?
    - How does the approach to investigations/interventions for more traditional, in-person actions compare to those online?
- When does online behavior, including bullying, threats, and self-harm, rise to the level where school leaders should involve law enforcement?
    - If law enforcement is engaged, what information is appropriate to share?
- What potential harms may result in addressing all monitoring system alerts with students?
    - Which factors differentiate the responses to each alert described?
    - What considerations need to be defined to assist leaders in alert responses?
    - Should some alerts be removed from the system?

- Under what conditions should school personnel get involved with potential bullying situations?
    - What kinds of notification trigger required responses, and how does the fact that the behavior or communication occurs outside of school hours and/or off of school property affect when and how a school responds?
- When cyberbullying allegations are lodged, what approaches (search, questioning, sharing of information/data) are appropriate for school personnel to take before communicating with families, and what approaches must be avoided or reserved for post-consenting processes?
- Consider the different roles of the school staff (teacher, school counselor, administrator), what actions and duties are within the purview of each role?
    - What goals, ethical considerations, policy and privacy constraints, and roles are appropriate for each personnel?
    - Where might these goals, ethical considerations, policy/privacy constraints, and roles overlap or conflict?

From the Evidence Vault:

- Ansary, N. S., Elias, M. J., Greene, M. B., & Green, S. (2015). Best practices to address (or reduce) bullying in schools. *Phi Delta Kappan 97*(2), 30-35.
- Barnes, K. (2015). The challenge of data privacy. *Educational Leadership 73*(3), 40-44.
- Englander, E. (2019). Looking at bullying in context. *Educational Leadership 7*(2), 54-58.
- Willard, N. (2011). School response to cyberbullying and sexting: The legal challenges. *Brigham Young University Education and Law Journal 1*, 75-126. https://heinonline.org/HOL/Page?handle=hein.journals/byuelj2011&div=7&g_sent=1&casa_token=&collection=journals#

In the News / In the World of Practice:

- Hickey, M. (2022, April 25). A 15-year-old boy died by suicide after relentless cyberbullying, and his parents say the Latin School could have done more to stop it. CBS Chicago. https://www.cbsnews.com/chicago/news/15-year-old-boy-cyberbullying-suicide-latin-school-chicago-lawsuit/
- Johnson, A. F. (2018). When can you search a student's phone? *THE journal: Transforming education through technology*. https://thejournal.com/articles/2018/03/12/when-can-you-search.aspx
- Oei, T. (2009, April 19). My students. My cellphone. My ordeal. *Washington Post.* https://www.washingtonpost.com/wp-dyn/content/article/2009/04/17/AR2009041702663.html
- Lehrer-Small, A. (2022, May 25). Does your school have a 'slander' account? *The 74.*

https://www.the74million.org/article/does-your-school-have-a-slander-account/

Data Privacy and Compliance Considerations

The above scenario presented some complicated intersections between privacy, ethics, and the district's obligations around student safety. It is the administrator's job to not only develop the knowledge of laws pertaining to these situations but also to provide resources to those best positioned to provide advice and mentoring. School principals need to understand the legal intersections related to device privacy, student safety, bullying allegations, and concerns about potentially sensitive private information, but school principals cannot have encyclopedic knowledge. When situations get complicated, leaders should review policy and procedures and reach out for guidance when unsure how to proceed.

A few considerations can help guide leaders regarding how they approach these types of situations, though it is critical to keep in mind that each case must be assessed independently based on its own set of facts. With regard to student first amendment rights, in the historic 1969 Supreme Court case *Tinker v. Des Moines*, the court held that students do not "shed their constitutional rights to freedom of speech or expression at the schoolhouse gate." Although this ruling stands and indicates that student speech is protected, this is not an absolute right. The court ruled that schools are justified in suppressing student speech if the conduct in question would "materially and substantially interfere" with school operations (see Tinker v. Des Moines). Since then, courts have wrestled with how to define this standard and more recently, how to determine what is within the school's purview in the context of a digital classroom.

In June of 2021, the Supreme Court revisited this issue in the case of *Mahanoy Area School District v. B.L*. A student was disciplined for posting on her personal social media account outside of school hours and off school premises using profane language about her frustration over not making the varsity cheerleading team. The court ruled in favor of the student, but in a limited capacity. "Given the many different kinds of off-campus speech, the different potential school-related and circumstance-specific justifications, and the differing extent to which those justifications may call for First Amendment leeway, we can, as a general matter, say little more than this: Taken together, these three features of much off-campus speech mean that the leeway the First Amendment grants to schools in light of their special characteristics is diminished. We leave for future cases to decide where, when, and how these features mean the speaker's off-campus location will make the critical difference" (see Mahanoy Area School District v. B.L).

This decision made it clear that there is no bright line rule. However, it also established that even if student conduct happens only off campus and outside of school hours, if the behaviors cause dangers or substantial disruptions during the school day, then school personnel are on notice that they must investigate and, likely, act (see Valerio Dominello & Hillman, LLC, 2021). In a case where the parties are known, are students at the school, and where actions suggest escalation, a thorough and careful investigation of facts is warranted. When districts adopt these types of student monitoring tools, it is critical that they consider what type of content is being captured, whether the tools are monitoring outside of school hours, and who has access to alert as capturing and storing this information may create a duty for the school to act.

School personnel must also be cautious with what may constitute or be interpreted as “searches” of students' personal devices (see Johnson, 2018). Even if a staff member does not consider their actions as conducting a “search” of a student’s phone, it could be construed as such later, especially if matters escalate to result in discipline. A safer approach would be to search using a school-owned device if possible. If the information is only accessible through a student’s personal device, it is advised that districts develop a policy and procedure with guidance from their legal counsel.

When investigating student behavior that may involve sexually explicit content, be it a report of inappropriate texts or internet searches, staff should be cautious not to download or access images that could themselves constitute pornography. Although well-intended, efforts to capture evidence for transmission to law enforcement have landed school personnel in hot water, as the downloading and storage of specific images (i.e., those constituting child pornography) is illegal, no matter the stated intent (see NPR, 2009; Oei, 2009). A safer practice here is to contact law enforcement and district leaders as soon as school personnel see any hint of such material to ensure that any evidence is collected in a responsible and legal manner.

There is an element of these scenarios that reaches into the area of potentially sensitive information. Of course, the primary analysis must focus on what disclosures are required or prohibited, and the course of action should center on the student’s well-being. That, however, is not always easy to decipher. For example, if a student’s search history reveals that the student is being abused at home and contemplating suicide, careful consideration of the first steps is warranted based on the specific situation. This may also be true if student self-harm or bullying is discovered to be associated with their sexual orientation, which is unknown to the parent/guardian. It is critical for school personnel to remember that capturing and storing student information and any documentation associated will become part of the student’s education record, which parents or legal guardians have the legal right to inspect.

There are some narrow exceptions, including state laws that allow records kept by licensed school counselors to be withheld from the student's education record. For example, in Texas, these records may be withheld “only if the records are kept in the sole possession of the counselor, are used only as the counselor’s personal memory aid, and are not accessible or revealed to any other person except a temporary substitute for the counselor,” and only if the counselor “determines that release” of the record(s) “would be harmful to the patient’s physical, mental, or emotional health” (T.E.A., 2022, FAQ #7). Of course, recent legislation in some states would seem to strengthen parental rights to access all records, unless the parent is the subject of a criminal investigation regarding a crime committed against the child (see, for example, Arizona’s 2022 House Bill 2161), which is why it is critical for school leaders to stay up to date on legislation that affects privacy in schools and with regard to school records and data collection.

In the scenario presented, any screen captures that would be used as evidence in the investigation would clearly be accessible by and available to the student’s parents, as they were not made in a counseling setting nor would be records kept in the sole possession of the counselor. However, comments made during discussions with students, if not captured in a school record or pertinent to the investigation, may not be considered part of the education record. In such situations, leaders should examine all legal and policy requirements and, when in

doubt, come down on the side of student safety.

In the vendor threat monitoring service scenario the determination must be made if this constitutes a "health or safety emergency" under FERPA to disclose information from a student's education record, in this case, to the police. It is important for school administrators to understand if the contracts and agreements for threat monitoring services give the vendor the authority to disclose threats to the police. Schools have a requirement under FERPA to record this disclosure in the student's education record.

Finally, there is the question of what images or information can be shared with whom. If the media posts are public, there is little constraint on showing them to any of the parents involved, particularly if the pictures are used as evidence of the concern and/or when trying to enlist families in discerning who operates the accounts in question. Any reports made by the students involved or school personnel can only be shared after personally identifiable information is fully redacted, and only in circumstances where the records are located in the files of those parents' minor children. Information solely in the file of another student should not be shared with other families.

Ethics and Norms

In most cases, once school personnel notice bullying or student safety concerns, policies almost always require further action and reporting. There may be variances in where and how these actions and reports flow, or what documentation is preserved where all school districts should have policies enacted. One way to violate ethical and legal duties is to brush off such concerns or simply excuse "teenage behaviors" as a rite of passage.

Bullying (in person or via social media or other digital means) is not a rite of passage; in fact, bullying has been associated with increased risks for suicidal thoughts and attempts in adolescents (NIH, 2022). Simply ignoring or minimizing an issue, whether noticed first by an adult (as in some scenarios) or by other students, as in the last scenarios, could increase the risk to a student's life. Educators have ethical and legal obligations to act on behalf of the student being victimized, and leaders have ethical obligations to create and sustain schools characterized by healthy, knowledgeable practices around digital citizenship, digital safety, and healthy relationship-building.

Leadership Practices & Data Use

Sometimes leaders are called upon to investigate and assign consequences; at other times, investigations may lead to restorative practices, counseling, or educational interventions. Still, at other times, allegations of cyberbullying or bullying (and other forms of harassment or mistreatment) may result in a mixture of some or all of these. Much depends on the nature, severity, and pervasiveness of the allegations and the age and developmental levels of the students involved. For these reasons, leaders should stay current on legal requirements and policy updates from their school districts, particularly as it involves student records privacy and disciplinary investigations. This is a difficult part of the leader's job: There are "teachable moments" where school personnel have the ability to bring families and students together to

repair or better relationships in ways that benefit students, but the personnel has to go about this in a thoughtful way that neither releases private data or information to parties to whom such access has not been granted, nor re-victimizes the subject of the original bullying/cyberbullying act.

One approach leaders can–and should–undertake is to be proactive about digital citizenship and safety, and to ensure a comprehensive curriculum that addresses digital citizenship, digital privacy, safety with technology, and protection from and reporting of cyberbullying is implemented schoolwide and is modeled by school personnel. Students, of course, need to be engaged in these lessons. Still, parents and families also need to be engaged around the benefits and potential dangers of rapidly evolving and emerging technology. Sometimes parents and families simply do not know the major dangers, or new risks to their children, and need strategies and tools to engage with technology in safer and more responsible ways. Common Sense Media (2020) is but one example of a comprehensive K-12 program that spirals six key topics throughout lessons (Media Balance & Well-Being; Privacy & Security; Digital Footprint & Identity; Relationships & Communication; Cyberbullying, Digital Drama, & Hate Speech; and News & Media Literacy).

School leaders are also responsible for ensuring that all educators (faculty, staff, and other employees) understand how they respond when students complain about mistreatment or safety concerns. Educators need to understand not only their ethical and legal obligations to respond but also the need to have a clear understanding of what procedural steps to take, or not take. However, when considering active monitoring of online activity and correlating alerts, leaders should carefully consider what activity alerts are appropriate. When alerts are received, staff have an obligation to review and determine action. If, for instance, an assistant principal receives alerts for all blocked searches conducted by a student, regardless of safety/risk level, reviewing and possible student conversations of those alerts could prove overly burdensome and detrimental to trust and relationships in the building.

Educators need to clearly understand that what they document about a student, whether in an email, a text, a grade book, a student information system, or a file is almost *always* accessible and available to the parent/guardian on request. FERPA makes such records available except under the narrowest and rare circumstances, and even then, only in situations involving legal requirements (e.g., subpoenas, warrants) or with very specially licensed personnel. For *most* school employees, they need to understand that if they document it in a student's record, or in a record about a student, it is fair game to be reviewed by the minor child's parent or guardian. This can give way to moral and ethical considerations when that information could increase the potential danger of student harm at home (child abuse, sexual abuse, sexual orientation). Although FERPA does not require the proactive notification of data in an education record, state laws may.

References and Resources

- Common Sense Media (2020). *Common sense education: Digital citizenship curriculum overview.* https://www.commonsense.org/education/digital-citizenship/curriculum
- Future of Privacy Forum. *Student privacy primer.* (2021, October 5)..

https://studentprivacycompass.org/resource/student-privacy-primer/

- Johnson, A. F. (2018). When can you search a student's phone? *THE journal: Transforming education through technology*.
- National Institutes of Health (2022, July 12). Cyberbullying linked with suicidal thoughts and attempts in young adolescents. *NIH Research Matters.* https://www.nih.gov/news-events/nih-research-matters/cyberbullying-linked-suicidal-thoughts-attempts-young-adolescents
- NPR (2009, April 28). Assistant principal vindicated of 'sexting' charges. https://tinyurl.com/53rcp5ks
- Oei, T. (2009, April 19). My students. My cellphone. My ordeal. *Washington Post.* https://www.washingtonpost.com/wp-dyn/content/article/2009/04/17/AR2009041702663.html
- Park, J., Cotto, J., Waller Curtis, A., Klein, C. Reddy, A., Siegl, J, Sollberger, A., Triplett, J. & Vance, A. (2021, January 12). *Student privacy communications toolkit: For schools & districts.* Future of Privacy Forum. https://studentprivacycompass.org/resource/student-privacy-communications-toolkit-for-schools-districts/
- Texas Education Agency (T.E.A.) (2022). *School counseling FAQs.* https://tea.texas.gov/academics/learning-support-and-programs/school-guidance-and-counseling/school-counseling-faqs
- Trujillo-Jenks, L., & Jenks, K. (2015). *Case studies on safety, bullying, and social media in schools: Current issues in educational leadership.* Routledge.
- Valerio Dominello & Hillman, LLC (2021, December 8). The First Circuit Court of Appeals holds that "off campus" cyberbullying by students can be a basis for discipline without violation the First Amendment or the Massachusetts Student Speech Statute. https://vdhboston.com/the-first-circuit-court-of-appeals-holds-that-off-campus-cyberbullying-by-students-can-be-a-basis-for-discipline-without-violating-the-first-amendment-or-the-massachusetts-student-sp/

Facilitator's Guide: Online Activity & Threat Monitoring

Teaching Notes and Considerations for Scenario Facilitators:

In this scenario, leaders must consider multiple and intersecting aspects of school safety, bullying, technology, data, and information sharing, discipline, and communication. They also have to consider what roles data, data privacy, ethical data use, and decision-making play as they navigate the examples of monitoring and alerts presented. Scenario users may identify additional connections to data use, privacy, ethics, and leadership not addressed in the teaching notes. You are encouraged to engage in the exploration of those connections.

Extending Activities

- Expanding on alert #1 above with Clay and social media threats, the counselor who received the alert recently spoke with Clay about a sudden decrease in-class participation and assignment completion. The counselor decides to talk with Clay about the alert. During the discussion, Clay shows the counselor other posts and text messages with similar threats. Some posts and text messages are from two district high school students while others are from a student in the middle school. Many of the messages are during school hours. One comment implies that in-person bullying occurs in the school by the middle school student who attends with Clay. Roleplay the investigation into the bullying allegation.
    - How might the counselor or administrator appropriately capture screenshots of text messages and other social media posts?
    - Provide a clear rationale for the questions asked, information shared, and information redacted or withheld. Assess the alignment of your rationale with FERPA requirements and with your own district policy about bullying, discipline, school safety, or other pertinent issues.
    - Are the screenshots of the social media comments and text messages educational records? If so, at what point do they become records, and how might they be properly protected?
    - What information can be shared and under what conditions?
- After reading some literature on privacy and digital safety (see resources in this scenario, or go beyond with a brief Google Scholar search), develop a brief "do's and don'ts" list to help guide school personnel on what they can and cannot (or should/should not) do with different monitoring alerts. Be explicit in identifying situations or stages of concern where they must engage other personnel to ensure student safety (e.g., counselor, administrator, school resource officer).
- Visit with the school counselor and IT specialist to review which alert systems are currently used by the district. Explore alerts offered by the district's current vendor(s) that have not been adopted. Why has the district decided not to utilize the additional services/tools/alerts?

Using Online Resources While Protecting Student Privacy

Learning Objectives

- Outline the benefits and potential data privacy concerns regarding student use of online EDTech applications.
- Explain the pros and cons of the most common FERPA exceptions (school official and consent) for sharing data with an online EDTech vendor.
- Understand that in addition to FERPA, additional state-specific laws may apply to the sharing of student data with third-party EDTech vendors.
- Identify what processes need to be in place to facilitate the safe sharing of student data.
- Explain the risks of using unvetted web-based applications, including identifying sensitive data shared and collected.

Dr. Smith, the associate superintendent of curriculum and instruction, frequently conducts walkthroughs with each building principal. On these walkthroughs, they observe classroom instruction and discuss instructional methods used in the building. During a walkthrough at Little Oak Elementary, Dr. Smith observed a class of first-grade students using iLoveMath, an online math program he had not seen before. The students were highly engaged in a game-based competition of completing addition and subtraction problems. The program allowed students to earn points for speed, accuracy, and use of "power-ups" and displayed their rank compared to their classmates, each having a unique animal assigned to them.

Dr. Smith checked the district's online approved applications list and did not see iLoveMath on the list as either approved or denied. After the walkthrough, Dr. Smith met with Mr. Bridge, the principal at Little Oak, to debrief. He inquired about the teacher's use of iLoveMath and if it was used in other classrooms. The principal was unaware of the use and followed up with the teacher, Mrs. Cooper, a second-year teacher. Mrs. Cooper explained that iLoveMath was shared with her by a fellow teacher in the district, and she had assumed it was approved. She stated that she had signed up for the free website at the beginning of the year and that her students had used it for the past two months. All students were assigned a unique animal for their avatars. Although no student names were used for student logins, the teacher did have a dashboard where she could see the skill mastery, engagement level, and total time for each student by name.

Mr. Bridge appreciated Mrs. Cooper's understanding of the privacy and FERPA concerns regarding using iLoveMath. They reviewed the process of verifying if an app was approved and how to submit one for approval if needed. The two then submitted iLoveMath through the district's approval process.

Discussion Questions

- What data might be collected by iLoveMath through the students' site use?
- Review the observation of the students' use of iLoveMath. Is any FERPA-protected information collected or shared? Are student records being created by iLoveMath?

- Would any of this data be considered Personal Identifiable Information? If the teacher only enters a student's name, would the use of this site fall under Directory Information?
- Would the teacher's use of student IDs instead of names mitigate FERPA violations or data-sharing concerns? What if the teacher used a randomly assigned animal instead of a student's name/ID, or made up a different code number for each student (rather than using a school-issued ID number?)
- If students couldn't see the rank of other students, just their own rank, such as 8th out of 24, how might this impact privacy or ethical concerns?
- Would any parent permissions be needed for students to use iLoveMath, with or without district approval? When and under what conditions would parent communication about using the platform/app (simple notification or consent) be necessary or desirable?
- If you were the principal at Little Oak Elementary, what would you do next?

From the Evidence Vault:

- CoSN Student Data Privacy Toolkit Part 2: Partnering with Service Providers https://www.cosn.org/wp-content/uploads/2023/01/CoSN-Student-Data-Privacy-Toolkit-Part-2-0323_v5.pdf
- Zimmerle, J. C. (2021). Safe, sound, and private: Promoting data protection for students. *Computers in the schools 38*(1), 1-18. https://doi.org/10.1080/07380569.2021.1882203

In the News / In the World of Practice:

- Singer N. (2015, March 11). Privacy pitfalls as education apps spread haphazardly. The New York Times. https://www.nytimes.com/2015/03/12/technology/learning-apps-outstrip-school-oversight-and-student-privacy-is-among-the-risks.html
- The University of Chicago Department of Computer Science (2023, February 21). UChicago and NYU research team finds edtech tools could pose privacy risks for students. https://cs.uchicago.edu/news/uchicago-and-nyu-research-team-finds-edtech-tools-could-pose-privacy-risks-for-students/

Data Privacy and Compliance Considerations

Many online instructional resources collect data beyond what is entered by the student and/or teacher. In the scenario below, although it may appear that iLoveMath only has the student name and avatar, as that is all the teacher entered, the site is collecting student performance data and associating that data with the teacher and other students in the class. Data collected by this site may include student name, assigned teacher, math competency progress, time to answer each question, the accuracy of each math skill, student engagement, and time on task.

The definition of Personal Identifiable Information (PII) varies by federal regulation. Districts and schools must consider the definition of PII under FERPA, IDEA, and COPPA when determining if PII is being shared (see chart below). In addition, state and district policies may further define PII. It is also important to know what the district defines as Directory Information in its annual FERPA

notice. Although a student name is a direct identifier, it may also meet the definition of directory information. It is possible for data to be both PII and directory information, as long as that information isn't considered harmful if released, and the school checks that parents have not opted out of directory information disclosures. Since the site in this scenario tracks each student, it is reasonable to assume they are using cookies or other persistent identifiers. The data collected by the cookies may be considered PII by some districts, states, and COPPA.

FERPA 20 U.S.C. 1232g and 34 CFR Part 99	(e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; (f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or (g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.
COPPA Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505 Children's Privacy	Individually identifiable information about an individual collected online, including: (1) A first and last name; (2) A home or other physical address including street name and name of a city or town; (3) Online contact information as defined in this section; (4) A screen or user name where it functions in the same manner as online contact information, as defined in this section; (5) A telephone number; (6) A Social Security number; (7) A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier; (8) A photograph, video, or audio file where such file contains a child's image or voice; (9) Geolocation information sufficient to identify street name and name of a city or town; or (10) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

Ethics and Norms

A primary ethical concern in having students use "free" resources and even purchased apps and electronic resources/platforms is that without appropriate notifications and communication, students may end up "purchasing" the ability to use apps via data provided to systems for use, including data then used for marketing to students and families. Ethically, schools should not compel students or their families to share data without consent to use a resource that should be provided as part of a free public education. Perhaps a good reminder for school leaders is there is no such thing as a "free app." Developers are either paid for their work directly or "paid" for the data they can collect and then resell–to marketers, other developers, etc. Humans have the autonomy to choose how to spend their resources–including their data, so removing appropriate

vetting and informed consent processes from any decision-making process that results in unvetted, unapproved technology being used by students (or used by educators, but which requires the provision or sharing of student PII), in effect, strips students and their families of this autonomy.

School leaders have long leaned on permission slips for many school functions, from student participation in sports to field trips. This may indeed satisfy legal requirements, but school leaders should be mindful when relying on consent as the basis for sharing student data with a third party, such as an EDTech service, that even in the best of circumstances, it is unlikely that 100% of parents will sign and return a consent form. This may be because they have yet to receive the form, the form was not provided in their home language, they did not have time to return the form, they have privacy concerns or other reasons. Where consent is the basis for sharing data, schools cannot share data without a signed consent form, and this will inevitably create extra work for the teacher to create separate lesson activities for students that did not receive consent or may disadvantage students that are not able to use a tool and participate with their classmates in the lesson.

Ethically, leaders are responsible for following appropriate vetting procedures to mitigate risks posed by e-resources, including apps (whether paid or free), for communicating with parents, for training teachers and other staff about procedures, and for ensuring that, where needed, consent is received and maintained to reduce the risks of harms due to inappropriate data sharing or even of data breaches (Student Privacy Compass, 2023).

Leadership Practices & Data Use

Teaching with technology can be a wonderful, value-added experience, but to do so requires consideration of several factors, from how the tech fits with pedagogical approaches and content standards, to issues of use and accessibility, to appropriate vetting to protect student privacy (Garcia & Nichols, 2021). When encouraging teachers to engage with technology for instructional purposes, leaders have to equip teachers to use the tech appropriately. Still, they also have to help them develop an understanding of processes required to vet apps/e-resources–including when consents are or should be collected–and why these processes are critical in mitigating potential risks to students.

Leaders should also ensure appropriate training so that all school staff are fully aware of their responsibility to protect student data and follow the applicable laws and school policies. This is particularly critical in an era where well-intended leaders, teachers, and staff may want to try "innovative" ideas using new technologies or be more inclined to use "free" services recommended by their peers. It's also important with paid apps, because teachers often reach into their own pockets when they believe a resource could benefit their students, but budgetary constraints stand in the way. Teachers must understand that while the budget may be an obstacle in the evening out the playing field for students, the dangers that can attach to some tech tools make it well worth the time and effort to seek approvals for apps through appropriate district channels.

Building and district leaders are often faced with the challenge of working through unexpected

situations. In this scenario, a teacher was unknowingly using an unapproved resource. The climate/culture of the district and building may impact how this scenario is addressed. Possible actions may include:

- Ensuring that the teacher no longer uses the app until fully vetted and approved.
- Retraining or otherwise reminding other teachers about policies surrounding the use of apps and other e-resources. After all, since the app was recommended to Mrs. Cooper, other teachers in the building (or district) may be using it or other unvetted resources.
    - A notice may need to be sent to all teachers in the building and/or communication during grade-level or staff meetings.
    - The leader may consider notifying other principals of the potential use of the app in their buildings.
- Providing teachers with updated information on apps and other resources that are already vetted and approved for use. Teachers adopt resources in an effort to achieve specific instructional goals. The use of unapproved apps may result from a lack of awareness of approved applications. The principal (or instructional leader) should assist teachers with finding approved resources to accomplish their instructional goal(s).
- If the app is denied through the district's approval process, the teacher, and principal, should ensure that all student data is removed by the vendor.
- The principal should consider facilitating building professional development around the app approval process, the use of only approved apps, how to verify if an app is approved, and privacy concerns with unapproved apps.

Finally, leaders need to remember that onboarding/training about resource adoption/use/purchasing policies needs to be ongoing so that as educators enter and exit the system, those coming into the system understand the appropriate processes for resource adoption and use. Leaders also need to ensure that persons who exit systems are removed from being able to access apps or other electronic systems that could provide inappropriate access to student PII. Working with IT and HR to ensure that those who leave systems have access to any systems (including apps and resources) accessed electronically is an important component of protecting student privacy.

References and Resources

- Garcia, A. & Nichols, T. P. (2021). Digital platforms aren't mere tools–they're complex environments. *Phi Delta Kappan 102*(6), 14-19.
- Park, J., Cotto, J., Waller Curtis, A., Klein, C. Reddy, A., Siegl, J, Sollberger, A., Triplett, J. & Vance, A. (2021, January 12). *Student privacy communications toolkit: For schools & districts.* Future of Privacy Forum. https://studentprivacycompass.org/resource/student-privacy-communications-toolkit-for-schools-districts/
- Student Privacy Compass (2023). *Best privacy practices for using apps in the classroom.* https://studentprivacycompass.org/audiences/educators/using-apps-in-the-classroom/

- Privacy Technical Assistance Center (2014, February). *Protecting student privacy while using online educational services: Requirements and best practices.* U. S. Department of Education. https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf
- Privacy Technical Assistance Center (2016, March). *Protecting student privacy while using online educational services: Model terms of service*. U. S. Department of Education. https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-model-terms-service
- Privacy Technical Assistance Center (n.d.). *I want to use [an] online tool or application as part of my course. However, I am worried that it is a violation of FERPA. What should I do?* U. S. Department of Education. https://studentprivacy.ed.gov/faq/i-want-use-online-tool-or-application-part-my-course-however-i-am-worried-it-violation-ferpa

Facilitator's Guide: Using Online Resources While Protecting Student Privacy

Teaching Notes and Considerations for Scenario Facilitators:

In this scenario, leaders must consider aspects of creating and communicating appropriate school policies and providing effective coaching to teachers –both of which are important components of school leadership–while keeping in mind intersecting laws, policies, and best practices related to data, information, and student privacy. While scenario users may identify additional connections to data use, privacy, ethics, and leadership not addressed in the teaching notes, in what follows, we point out several areas that facilitators may choose to highlight as they lead groups in debriefing the "Using Online Resources While Protecting Student Privacy" scenario.

Extending Activities

- Mr. Bridge and Mrs. Cooper worked together to submit a software approval request using the district's online form. The approval process has a flow chart and questions the two work through. When they get to the question, "Does the resource require parental consent?" they review the privacy policy and terms of service and find that, in fact, it does require parental consent for use by students under the age of 13.
    - Why might iLoveMath require parental consent for students under the age of 13?
    - What are the risks of allowing students under 13 to use the resource without parental consent?
    - Can the district/school use the School Official exception under FERPA if direct parental consent is required?
    - The curriculum team has determined that this resource aligns with the curriculum, and is engaging, and would like to include it in the approved applications list. How might the district approach compliance?
- In the scenario, iLoveMath collects the student's name, shown only on the teacher dashboard. Is the use of the student's name the main factor when considering FERPA and the creation of a student record? Would iLoveMath still create student records if the teacher only saw the avatars and no student names were entered into the system?
    - What if the students could not see each other's avatars, so the student associated with each avatar was only known by the teacher?
    - Consider the fact that the teacher can still identify each student's record due to the use of an avatar (other systems may use pseudonyms instead of avatars).
- Examine the process for your school/district to ensure that all curricular resources, including free electronic resources, meet ethical and legal compliance.

- What is the process by which approvals/vetting is conducted for apps or other electronic resources that campus educators may want to use?
- What steps are taken when an unapproved resource is found to be in use?
- What training/communication is in place to ensure all necessary staff are aware of the process and why it is in place? If there is none, develop a brief training to meet this need.

Data Sharing with Law Enforcement

Learning Objectives

- Explain policies and procedures that must be considered or followed when responding to requests by law enforcement, and the courts.
- Describe the appropriate pathways for law enforcement officials to access educational records, including when and under what conditions school based LEOs may have access to educational data systems and the records stored in those systems.

One afternoon, Deputy Rex walks into the main office at Burke River Middle School (BRMS). He is not assigned to the school as an SRO but often has responded to a few calls at BRMS over the past few years. He is familiar with most staff at BRMS.

"Hey there, Mrs. Taylor," he says, walking up to the attendance window. "I need to see if Jackson Daniels is in class today, and whether he was here yesterday and last Friday. Can you help me verify whether he was here or absent?" His mom says he was here those days and is here today, but you know they've had some problems at the corner store with some shoplifting and the clerk working there today thinks he recognized Jackson this morning and the other afternoon, so I'm just trying to follow up. Normally it's not on my priorities list, but there was also some vandalism around that time so we're just chasing down anyone who might have some information. If he is here, I'd appreciate a chance to talk with him–of course, only with Officer Stanley present."

At the mention of talking to the student, however, Mrs. Taylor's fingers slowed down–they had been quickly tapping at the keyboard, looking up Jackson's history.

"Oh, you know, I'm not so sure about protocols here. Usually, if there's a question related to an investigation outside of the school, we have some paperwork, you know. Like a subpoena or something. Do you have that?"

Deputy Rex responds. "I'm actually hoping to keep it from becoming a big deal–that's why I was hoping to just talk to Jackson kind of off the record to see if he knows anything first."

"Well, let me check with Officer Stanley, just to be on the safe side," Mrs. Taylor responds. She tries to reach Officer Stanley on the radio but doesn't get a response. A few minutes later, Mr. Bradley, an Assistant Principal, walks in. "Officer Stanley is in a meeting with a parent, but I heard your call on the radio," he says.

"If it's a problem I can just wait until Officer Stanley is free," Deputy Rex says. "She can look it up, I think, on her system. I think all the SROs have admin access." He pauses. "Of course, I'm not trying to get any of you in hot water either, so if you really need a subpoena, I can go get one–it just takes forever so I was hoping to figure this out faster and without getting the courts involved if it isn't necessary. Just trying to avoid Jackson's name getting put on stuff in the system if there's no need for it"

“No, no,” responds Mr. Bradley. “It’s not that big of a deal. Of course, I can verify the attendance for you,” he says, typing into the attendance office computer. “It looks like he is here today, though he was about 20 minutes late for first period, and he was present the other two days, though he left at lunch on Friday–the exit log doesn’t show a reason.” Mr. Bradley scribbles the dates and Jackson’s attendance info onto a post-it note and hands it to Deputy Rex. “But with Jackson being a minor, I can’t let you talk with him without first calling a parent and getting permission– If you’d like to talk with him, I can go give his mom a call if you can wait a bit.”

“No, no need,” responds Deputy Rex. “This is helpful information already. He probably isn’t the kid the clerk saw today, because the times for this morning don’t match up. Of course, that absence last Friday may be a problem, but I can check back later if there’s anything else.” Deputy Rex thanks Mrs. Taylor and Mr. Bradley for the information, and waves as he leaves the office, notes in hand.

“So,” Mrs. Taylor says, “Should I call Jackson’s mother and tell her that the sheriff’s office was here asking about Jackson’s attendance?”

Mr. Bradley pauses. “It sounded like he already talked with her, but yeah, I think it couldn't also hurt to let her know. We should probably also inform Officer Stanley when she’s out of her meeting.”

“I’ll email her about it,” Mrs. Taylor responds. “I’ll go ahead and copy you and Principal Sparks, in case you need it for your records.”

Discussion Questions

- How should Mrs. Taylor (and later, Mr. Bradley) have handled the inquiry from Deputy Rex?
- To what data should Officer Stanley have access to via the district student information system, and which data (if any) should be restricted in some way? Explain your rationale.
- If the situation were altered, and Deputy Rex called Officer Stanley directly to inquire about Jackson’s attendance on the dates and times in question, would Officer Stanley be in the right to release that information? Why or why not?
- Under what circumstances should the school provide Deputy Rex with the information being sought?
- This case presents a non-emergency situation; if Deputy Rex were seeking information in an emergency situation, would the school be authorized to release the information? If so, what kinds of situations constitute “an emergency” and what kinds of data may be shared in such a situation and to whom?

From the Evidence Vault:

- Cole, J. P. (2021, May 24). *The Family Educational Rights and Privacy Act (FERPA): Legal Issues.* Congressional Research Service, Document R46799. https://files.eric.ed.gov/fulltext/ED614263.pdf

- Layton, D., & Shaler, G. (2019). *School-based policing in Maine: A study on school resource officers in Maine's public schools.* Maine Statistical Analysis Center. https://digitalcommons.usm.maine.edu/cgi/viewcontent.cgi?article=1002&context=maine_statistical_analysis_center
- Montes, A.N., Mears, D.P., Collier, N.L., Pesta, G.B., Siennick, S.E., & Brown, S.J. (2020). Blurred and confused: The paradox of police in schools. *Policing 15*(2), 1546-1564.
- Sugarman, J. (2019, June). Legal protections for K-12 English learners and immigrant-background students (Issue brief). Migration Policy Institute, National Center on Immigrant Integration Policy. https://www.immigrationresearch.org/system/files/Legal-Protections-for%20K-12-English-Learner.pdf

In the News / In the World of Practice:

- Bedi, N. & McGrory, K. (2020, November 19). Pasco's sheriff uses grades and abuse histories to label schoolchildren potential criminals: The kids and their parents don't know. *Tampa Bay Times.* https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/school-data/
- Creel, K. & Dixit, T. (2022, September 15). Privacy and paternalism: The ethics of student data collection. *The MIT Press Reader.* https://thereader.mitpress.mit.edu/privacy-and-paternalism-the-ethics-of-student-data-collection/
- Estes, A. (2022, July 7). Amid school violence, frustrated law enforcement officials say Boston Public Schools leaving them in the dark. *Boston Globe.* https://www.bostonglobe.com/2022/07/07/metro/school-violence-returns-prepandemic-levels-frustrated-law-enforcement-officials-say-boston-public-schools-leaving-them-dark/
- McGrory, K., Bedi, N., & Ellenbogen, R. (2021, January 19). Congressman urges probe of Pasco school data program. *Tampa Bay Times.* https://www.tampabay.com/investigations/2021/01/19/congressman-urges-probe-of-pasco-school-data-program/

Data Privacy and Compliance Considerations

In the scenario as written, it is clear from Deputy Rex's statements that he does not have a subpoena or court order for Jackson's records, and the school has no written release from Jackson's parent or legal guardian to allow the release of the information sought. In fact, Deputy Rex's request seems almost casual and off the cuff, and the school has no way of knowing whether the purported shoplifting investigation is, in fact, the reason for the request. Deputy Rex is requesting the disclosure of an educational record for a law enforcement purpose, rather than for an "educational purpose directed by the school" (Future of Privacy Forum, 2021, p. 8). Thus, the request will not fall under the "school official" exception of FERPA, and nothing suggests the request is made in response to a situation that would justify the release of information under the health and safety emergencies exception to FERPA.

Deputy Rex indicates that he has talked with Jackson's mother. Still, the school has obviously received no notice from the parent that she is approving the release of the information related to

Jackson's attendance. Without signed consent to release the information, and in the absence of another FERPA exception that would permit the release of information, the school may not release information from Jackson's educational record (in this scenario, his attendance data) to Deputy Rex. In this scenario, Mrs. Taylor nearly erred in that she began processing the request until Deputy Rex's additional inquiry about interviewing Jackson caused her to pause and call for further direction (a good move when any employee is uncertain). Unfortunately, Mr. Bradley compounded the problem by failing to follow what should be established protocols. Mr. Bradley should not have looked up the information and provided it to Deputy Rex; doing so without proper authorization violated FERPA and could be the basis for a complaint.

Sometimes law enforcement officers (LEOs) work so closely with the school–or may even work for the school (as school resource officers or as part of a district-based security unit), they may function largely as members of the school faculty and staff. But when and under what conditions they may have access to student PII is determined by the intersection of the context (emergency or non-emergency), the purpose/use of the record(s) sought (for "school official" purposes or law enforcement purposes), and whether the presenting LEO is authorized to access the record (i.e., by subpoena, or by written consent of the eligible student or parent/legal guardian) (see FBI, n.d.).

It is also important to recognize that school officials may be confused in that "directory information" (which can be disclosed, unless Jackson's family has opted out of the sharing of directory information) includes "dates of attendance," which can seem to match Deputy Rex's request. However, FERPA regulations define "dates of attendance" as "the period of time during which a student attends or attended an educational agency or institution" (PTAC, n.d., "Glossary"). By this, the law means "Student X attended from Fall 2018 through Spring 2022," and not the granular type of day-to-day (in this scenario, even minute-by-minute) physical presence of the student. The school would act appropriately in sharing that information with Deputy Rex. Of course, if Jackson's family opted out of sharing directory information, the school would not be able to share that information. However, in this scenario, Deputy Rex already knew Jackson was a student at Burke River, and was requesting more granular information that comprised an educational record.

Three final notes as to legality/privacy apply. First, it would not have mattered if SRO Stanley requested in lieu of or for Deputy Rex. Though employed by the school through an MOU, using an educational record for law enforcement purposes, rather than for educational purposes, and then disclosing it to law enforcement, would not be permitted. Even as an SRO, Officer Stanley must follow legal requirements for accessing attendance records. What's more, the school should clearly delineate which data systems, and under what circumstances, Officer Stanley should be able to access. [It is unclear whether Deputy Rex's assertion that Officer Stanley has administrator-level access to the student data system is accurate, but this needs to be explored and, if necessary, addressed.] Working at the school does not create an unfettered right to all student data; like any other employee, Officer Stanley should only access student records in ways appropriate to her role, connection to the student, and purpose for accessing the records.

Second, subject to particular exceptions (typically situations where doing so is prohibited by a court order), "schools and districts must maintain a record of each request for access to and each disclosure of PII from the education records of each student, as well as the names of State and

local educational authorities and federal officials and agencies listed in 34 CFR § 99.31(a)(3) that may make further disclosures of PII from the student's education records without consent" (PTAC, 2019, p. 9). Further, that documentation must include who requested or received PII, "the legitimate interests the parties had in requesting or obtaining the information (i.e., under which exception to FERPA's general written consent requirement the disclosure was made" (PTAC, 2019, p. 9). Therefore, when making a permitted disclosure, the school needs to record what data they released to Deputy Rex, and for what purposes it was released. Quite obviously, if Mr. Bradley had worked through this process before looking up and releasing the information, it might have become apparent that the request fell outside of any legal exception to FERPA, and it might have saved him from his eventual error.

Third, if Officer Stanley had presented a subpoena, the school is required to make a reasonable effort to notify the student's parent in advance of providing any information, so that the parent may exercise their right to seek protective action.

Ethics and Norms

Cooperation across agencies can be mutually beneficial, but students' personal data must be protected; having or wishing to maintain a friendly relationship with law enforcement is not a reason to violate student privacy laws. Legally, and ethically, student data is private by default and can only be shared with parental consent, or under a limited number of exceptions (for example, when required via subpoena). School employees may feel torn or have a sense of internal strife when they decline a request for information from first responders that do not meet privacy/disclosure requirements. However, leaders need to ensure that all employees know that acting in accordance with laws–including privacy laws–is actually respecting the law, and is not a statement of how the employee or the district feels about the officer themself. There are moments in leadership where leaders (and all employees) have to say 'no' to someone (a colleague, a student, a parent, or a family member) they otherwise like and with whom they want to remain on good terms. Requests for educational records (and to be clear, detailed attendance records are educational records), may be one of those occasions.

Mr. Bradley could have navigated this scenario legally and ethically by explaining the procedures to Deputy Rex and noting they would need either a legal request (subpoena) or written consent from Jackson's parent or legal guardian. Mr. Bradley did make at least one good decision in this scenario: He declined Deputy Rex's nudge to pull Jackson from class for an 'interview' unless he first obtained parental consent; in doing so, readers of the scenario also learn something positive about Officer Stanley–that is, that she has worked to instill knowledge of appropriate procedures when any law enforcement officer–herself included–has need to talk with a student.

It is possible that declining Deputy Rex's request could lead to negative consequences or a less amicable relationship between the sheriff's office and the school, or between Deputy Rex and the person who denied the request. But doing the right thing–legally and ethically–is never without risk. When in doubt, educators need to keep in mind a primary ethical duty to protect students, and they must also remember that cooperative agreements between schools/districts and law enforcement agencies are supposed to be just that: cooperative. The presence of an agreement does not make the school an arm of law enforcement, and school personnel should not be

pressed into positions where they are, in effect, stepping out of their roles as educators or school staff to access records to which LEOs are otherwise unauthorized to access.

Leadership Practices & Data Use

School leaders are responsible for protecting the rights of the students. This includes school safety and the protection of student information. Leaders should be knowledgeable about the processes and regulations that pertain to sharing student data with other agencies. They must know when a request is legitimate and appropriate. As Montes et al. (2020) note, FERPA "does not give officers the automatic right to access student records" (p. 1554). Leaders are responsible for building capacity in anyone with authority over or access to student PII and educational records so that employees know when and under what conditions information may be released. They also need to ensure appropriate processes and procedures (for example, how access to records must be logged, and how/where such logs are maintained) are in place, and that all employees are familiar with and abide by these procedures.

Given her uncertainty, Mrs. Taylor did the right thing by calling for assistance, though her first call should have gone to an administrator rather than Officer Stanley. It's very possible that Officer Stanley is both ethical and perfectly knowledgeable about appropriate records requests and access, and could/would have provided accurate guidance, but the request for assistance more appropriately resides with the chief operating officer of the school, which would be the principal or a designee. This aligns with the nature of the SRO's access to student data as a "school official" under the direct control of the school. with respect to the use of education records.

Unfortunately, the call for assistance was answered by an administrator who was either unfamiliar with student privacy regulations or was willing to provide the information outside of legal authorization to do so. Whether Mr. Bradley provided the information out of ignorance of the law, a desire to engage positively with Deputy Rex, or a combination of both, his decision could have ramifications for the school and district. Beyond a potential complaint, the decision will also likely erode trust and the possibility of a positive working relationship with Jackson's family (and other families, should Jackson or his parent share what happened with others in the community). Though Principal Sparks was not central to the scenario, the fact is that at least two employees under her supervision were either unsure about proper privacy protections or opted to ignore procedures; that responsibility resides with Principal Sparks, so it will be on her to address the problem with corrective actions. She should also report the breach of protocol to her supervisor.

References and Resources

- Federal Bureau of Investigation (n.d.). *Family Educational Rights and Privacy Act: A guide for first responders and law enforcement.* https://www.fbi.gov/file-repository/ferpa-guide.pdf
- Park, J., Cotto, J., Waller Curtis, A., Klein, C. Reddy, A., Siegl, J, Sollberger, A., Triplett, J. & Vance, A. (2021, January 12). *Student privacy communications toolkit: For schools & districts.* Future of Privacy Forum. https://studentprivacycompass.org/resource/student-privacy-communications-toolkit-for-schools-districts/

- Privacy Technical Assistance Center (PTAC) (2019, February). *School resource officers, school law enforcement units, and the Family Educational Rights and Privacy Act (FERPA).* https://studentprivacy.ed.gov/resources/school-resource-officers-school-law-enforcement-units-and-ferpa
- Stephen Sawchuk (2021) *School Resource Officers (SROs), Explained* (Education Week) https://www.edweek.org/leadership/school-resource-officer-sro-duties-effectivenessadd

Facilitator's Guide: Data Sharing with Law Enforcement

Teaching Notes and Considerations for Scenario Facilitators:

Scenario users will encounter and explore multiple applications of data privacy, data ethics, and leadership as they read, work through discussion questions, and engage in the suggested activities. While not all applications of data use, ethics, and privacy will be covered by these teaching notes, below we point out several areas that facilitators may choose to emphasize as they lead groups in learning with the "Data Sharing with Law Enforcement" scenario.

Extending Activities

- Place yourself in the role of Principal Sparks, reading Mrs. Taylor's email. What is your initial assessment, and what steps will you take next, regarding policies, procedures, or communication? Explain your response and your rationale.
- Do a quick "walking survey" of your campus. Ask employees what they would do if the school SRO or LEO asked for data/information on a student. Do responses fit with your expectations of how educators in your school would respond? Do the responses you receive align with policies and legal requirements? If not, how might you help faculty and staff align responses with such requirements?
- Sometimes school personnel may feel awkward redirecting requests from law enforcement, given that they want to support LEOs and maintain positive relationships with law enforcement agencies. To assist with this, consult your local policies and any MOUs and compose a script (or scripts) that help staff respond to requests in ways that are consistent with local, state, and federal laws and policies.

Student Health Information

Learning Objectives

- Explain the difference between health-related education records and medical records and the application of FERPA and HIPAA as they pertain to records maintained by schools.
- Identify potential data privacy concerns regarding student health information, including vaccination records and medical conditions.
- Outline the benefits, potential risks, or actual harms of collecting student health data as part of the curriculum.
- Identify when and under what conditions student health information may be released to persons outside of school employees with a legitimate educational interest.

The River School District serves a diverse population of students and families. Several schools have at least one student who requires the district to staff a nurse to provide direct care throughout the day. In addition, a new healthy living initiative has been implemented across the district. Students engage in various activities that promote physical and mental well-being. Over the past few years, there has been a growing concern among parents and staff about the privacy of their personal health information. Some stakeholders have expressed concerns that the district is violating HIPAA with its practices.

Below is a list of concerns brought to the district's attention. These concerns require leadership to consider if the actions and policies are legally compliant, ethical, and/or best practice.

- A new "Know Your Numbers" grant has been used to provide health monitors for every school. During PE class, students wear biometric monitors, numbered, and synchronized to an online app the PE teacher manages. Students begin by determining their baseline heart rate, then work with the teacher to set a target heart rate. The students use an online spreadsheet to record their steps, distance, heart rate, time at target heart rate, and oxygen levels throughout physical activity. Jonny's mom expresses concern about an online application tracking personal health information.
- Jack Smith, a student with severe allergies, was recently enrolled in Blue River Elementary. Before attending class, his 504 team met. Since Jack's allergies included food and environmental triggers, many activity-specific accommodations were implemented. Since young students are often taken by the hand by teachers working the bus line, Jack's mom requested that all staff be informed that he was to not be in contact with any scented products, including perfumes and lotions. In addition, special cleaners would be needed for any area Jack came in contact with as Jack was allergic to the school's standard cleaner. The 504 team asked Jack's mother if a letter could be sent home with all students in his class requesting that parents not send in scented lotions or hand sanitizers, and his mother agreed. During the next staff meeting, the principal addressed all staff to ensure they were aware of Jack's allergies and to be sure they did not accidentally expose him. On the first day of school, Jack's teacher held a class meeting to discuss a special friend in the class and how to keep him safe. Although Jack was not named, his use of medical

gloves and special soap was noticeable to all students. Lastly, Jack's teacher created a document for her sub with special instructions for Jack, this letter listed all of his allergies and detailed accommodations. She shared this letter with all the teachers in the building. The school counselor, who oversees 504 compliance, expressed concern that the team overshared with regard to Jack's condition with staff.

- Last month, a fight broke out between two high school students during dismissals. A school resource officer responded to the fight and yelled at nearby students to back up. A teacher noticed Jimmy, a nonverbal student with autism, and an assistant who works with Jimmy, near the group. The noise and unpredictability of the event appeared to agitate Jimmy, who began physical stimming (in this case, flapping his hands and beginning to pace quickly about the area). The officer noticed Jimmy and observed him becoming increasingly physically agitated and, in his pacing, inadvertently beginning to get closer to the officer and the students involved in the fight. The teacher noticed that Jimmy was pushing away from the assistant, who was trying to move Jimmy back from the area and also noticed the officer trying to both get control of the fight and ascertain why Jimmy was still approaching, despite verbal orders to back up. The teacher said loudly to the officer, "Officer! The tall boy in the blue jacket is autistic and nonverbal; he isn't aggressive and is just frightened, but he won't respond to you–we need to get closer to help him!" The student's assistant was glad the teacher jumped in to protect Jimmy and prevent any misunderstandings. Still, he was worried about the teacher sharing Jimmy's diagnosis in such a public way.
- Ms. Cricket, one of the visual art teachers at RRHS, began a six-week family leave in October. In her desk drawer, she left a binder of plans and information for the long-term substitute, Mrs. Lawrence. The week before the start of her leave, Ms. Cricket provided Mrs. Lawrence with a tour of the classroom, answered questions, provided a key to the desk, and walked Ms. Cricket through the sub binder of information kept locked in the desk. In the binder, immediately after each roster, is a list of students and notes related to the students, including particular program information and pertinent health information. For example, Aurora in the second period needs to be able to use her inhaler as needed; Jack in the fifth period has an Epipen that he may need in contact with nuts; and Ethan in fourth period has a seizure disorder. Ethan's seizure plan is also included in the binder.

Discussion Questions

General/Overarching questions:

- What factors should be considered to determine if HIPAA or FERPA apply?
    - At what point is student health information a FERPA record vs a HIPAA record? Can it be both?
    - Where does HIPAA or FERPA apply to these scenarios?
    - Which facts lend to that determination?
- Which actions might cause ethical or legal concerns?
    - How might you remedy those concerns?

- What processes, policies, or other safeguards (technology-based or physical) should be in place to ensure all personnel who need health information–including substitutes–have important information without compromising student data privacy?

For Situation 1:

- Assess the parent's complaint that Mr. Joshua's statements violated HIPAA. Was the parent correct? Why or why not?
- How should Dr. Manning reply to the parent? What, if any, communication should he engage in with Mr. Joshua and/or the superintendent in connection with the parent's email?

For Situation 2:

- Assess the legality of the school's communication:
    - Which communications were within the context of "legitimate educational interest" or "parental consent"?
    - Which communications may have exceeded what the school/staff allowed?
    - What documentation should be maintained regarding the different communications?
- What, if anything, constrains the school from ensuring Jack's safety while maintaining appropriate confidentiality? How might the school ensure compliance?

For Situation 3:

- Assess the teacher's actions in light of FERPA. Was the teacher justified in communicating with the responding officers about Jimmy's situation in a manner that revealed a diagnosis?
- How would the propriety of the teacher's actions be affected if the officer worked for an external law enforcement agency (for example, if the incident occurred on a field trip, or in a location where local law enforcement, rather than an SRO, responded to a call?

For Situation 4:

- Has Ms. Cricket acted appropriately in communicating student health information to Mrs. Lawrence? Why or why not?
- Could Ms. Cricket simply have given Mrs. Lawrence her access codes to the student information systems (instead of printing out/including health information in a binder)?

From the Evidence Vault:

The Center for Disease Control has developed guidelines for school vaccinations, requirements, and exemptions. Their website and those of the state education agencies and local education agencies should be consulted, as some state policies related to schools and vaccination or other health-related policies (e.g., asthma inhalers, EpiPens) may vary.

- Bugden, E.A., Martinez, A.K., Greene, B.Z., & Eig, K. (2011). *Safe at school and ready to learn: A comprehensive policy guide for protecting students with life-threatening food allergies.* National School Boards Association. https://adayinourshoes.com/wp-content/uploads/USDHHS-Food-Allergy-Guide.pdf
- Center for Disease Control. (n.d.). *School vaccination requirements and exemptions*. Retrieved from https://www.cdc.gov/vaccines/imz-managers/coverage/schoolvaxview/requirements/index.html
- Darden, E.D. (2013). Food allergies inject legal risk. *Phi Delta Kappan 95*(2), 70-71.
- Reddy, A. & Vance, A. (2020, March 20). *Student privacy during the COVID-19 pandemic.* AASA and Future of Privacy Forum. https://www.pasa-net.org/Files/Coronavirus/March23/StudentPrivacyFAQ3-20-20.pdf
- U. S. Department of Health and Human Services [DHHS] and U. S Department of Education [ED] (2019). *Joint guidance on the application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to student health records.* https://studentprivacy.ed.gov/sites/default/files/resource_document/file/2019%20HIPAA%20FERPA%20Joint%20Guidance%20508.pdf

In the News / In the World of Practice:

- Alltucker, K. (2023, January 12). 'This is alarming': Childhood vaccination rates drop as measles and polio outbreaks emerge. *USA Today.* https://www.usatoday.com/story/news/health/2023/01/12/childhood-vaccination-rates-drop/11039032002/
- Keierleber, M. (2023, February 22). Trove of L.A. students' mental health records posted to dark web after cyber hack. *The 74*. https://www.the74million.org/article/trove-of-l-a-students-mental-health-records-posted-to-dark-web-after-cyber-hack/
- Mayorquin, O. (2022, November 20). California school district to pay $15.75 million to settle suit over student asthma attack death. *USA Today.* https://www.usatoday.com/story/news/nation/2022/11/20/california-school-district-student-asthma-attack-settlement/10745499002/
- Ross, N. (2022, September 9). EpiPens now available for students at every school in the Lee County School District. *Fort Myers News-Press.* https://www.news-press.com/story/news/education/2022/09/09/lee-county-schools-gets-two-epipens-per-school-students/7948772001/

Data Privacy and Compliance Considerations

Despite several of the scenarios seeming quite complex, school leaders should take some comfort in knowing that public schools and school personnel very rarely fall under the auspices of HIPAA. Despite widespread confusion and unfortunate assumptions that anything related to health (including injury reports, vaccination information, and illness details) is "HIPAA-protected,"

this is not the case in most public schools. HIPAA governs “institutional providers of health or medical services, such as hospitals, as well as non-institutional providers, such as physicians, dentists, and other practitioners, along with any other person or organization that furnishes, bills, or is paid for health care in the normal course of business” (DHHS & ED, 2019, p. 5).

Unless the school is in a somewhat unusual situation where the school “provides health care to students in the normal course of business, such as through a health clinic,” the school is unlikely to be subject to HIPAA. Even those schools that do meet the statutory definition of a “HIPAA-covered entity” still do not have to comply with the HIPAA Rules If the only health records they maintain are “education records” or “treatment records" (DHHS & ED, 2019, p. 7). Federal guidance notes that typically, “The school is not a HIPAA-covered entity. The HIPAA Privacy Rule only applies to health plans, health care clearinghouses, and those health care providers that transmit health information electronically in connection with certain administrative and financial transactions. […] such as health care claims submitted to a health plan” (DHHS & ED, 2019, p. 7). Moreover, even in some cases where a school may bill Medicaid electronically, but only uses health information maintained within education records. The school is still required to comply with FERPA, not HIPAA. If a school is a HIPAA-covered entity, that is not a decision being made at the campus level; the kinds of medical billing using particular transaction methods and PII will be governed by persons with particular expertise within the district. When in doubt, school leaders should inquire of district-level medical personnel about HIPAA requirements, but in general, leaders should concern themselves primarily with safeguarding student health information contained in educational records (and which are subject to FERPA or, when related to a student who qualifies for special education services, to privacy regulations of IDEA).

In sum, in most cases, student health information maintained and used by the school will be considered “educational records” and therefore governed not by HIPAA, but by FERPA. This includes vaccination records, which are both “directly related to a student” and “maintained by an educational agency” (DHHS & ED, 2019, p. 4). When considering whether health-related information can be released, school leaders should ask the same questions they do when considering the propriety of any release of educational records. (1) Is the release of information to a school employee, contractor, or district with a legitimate need to know the information to safeguard and serve the child appropriately? If the answer is “no” then the information may only be released with written consent of the parent or legal guardian, or under court order. (2) Is releasing information necessary to mitigate an emergency situation? If “yes,” then the information may be shared with personnel (including law enforcement personnel) to mitigate the emergency–to the student or to others. For example, in Situation E, the teacher appropriately communicated with the law enforcement officer about Jimmy’s condition; not doing so could have immediately increased the risk to Jimmy, others, and potentially even the responding officers. While it is unfortunate that others were within earshot, the situation called for immediate and clear communication and did not provide time or space for more discrete communication.

Finally, it’s important to acknowledge that neither FERPA nor HIPAA prevents individuals (employees, volunteers, or even students) from disclosing their own health information. A few other notes specific to the scenarios posed above:

- In situation 1, “Know Your Numbers” grant, there have been no HIPAA violations. Again,

the public school is not subject to HIPAA (this might not be the case if this was a private school with a health clinic that was billing the cost of the monitors to individual student's private insurance, which in narrow circumstances could be subject to HIPAA). Since the school is collecting and maintaining the information and is disclosing them to a third-party app, they are definitely education records covered by FERPA, and the school must ensure that they are disclosed in an appropriate way. This is typically (and best) done using FERPA's school official exception, which requires that the third party:

1. Performs an institutional service or function for which the agency or institution would otherwise use employees
2. Is under the direct control of the agency or institution with respect to the use and maintenance of education records (usually through a contract)
3. uses the data "only for the purposes for which the disclosure was made"
4. and "Meets the criteria specified in the school or local educational agency's (LEA's) annual notification of FERPA rights for being a school official with a legitimate educational interest in the education records"

If all of these conditions are not met (e.g., no evidence of direct control), or the data is used for non-educational purposes (e.g., targeted advertisements) then there could be a FERPA violation.

- Situation 2 is a bit more complex; Jack's parents have the right to disclose their son's medical information as they see fit, to whom they see fit. Communicating about his medical condition might encourage other students (and staff) to take extra precautions that permit Jack to access the educational program most fully–a clear goal of IDEA's inclusion/least restrictive environment provision. Sending home such a letter is a common approach, and documents in the sole possession of a teacher that are shared only with a substitute are not considered Education Records. It would be important to consider if all teachers in the building have a need or legitimate educational interest in this information.
- Situation 3 presents a teacher with student health information likely governed by FERPA (as an education record) and IDEA (as part of a special education record). However, in an emergency, where a student's life or well-being is at imminent risk, educators can disclose information to keep the student safe. Of course, it would be nice if emergencies always happened privately or out of earshot of others. Still, in this instance, the teacher had to make a fast decision given a quickly changing (and emotionally charged) situation. The teacher's actions here align with the provisions of FERPA that permit disclosure without written consent in emergencies.
- Situation 4 demonstrates the importance of structures facilitating information sharing about health information. Though Ms. Cricket does not have written consent to share the students' health information with Mrs. Lawrence, she technically does not need it, as Mrs. Lawrence has a legitimate need to know to safeguard and serve the students appropriately.

There are pros and cons to the approach taken in this scenario. In terms of data privacy, it would still be better if the school had a process for sharing this information in more secure ways than in a physical binder (which could be misplaced and thus inadvertently shared with persons who do *not* have a legitimate need to know about the student's needs). In this situation, the binder was at least kept in a locked desk drawer and meets the definition of information that is not part of a FERPA record as it is kept in the sole possession of the teacher and shared only with someone such as a substitute. This is the preferred approach to sharing this data type in many schools, as long as appropriate communication, training, and security measures are taken.

An alternative would be to maintain this type of information electronically in a student information system that secured and controlled access to teachers and substitutes with a legitimate interest in the information. However, sharing one's password with a substitute would not be a good practice. This would likely violate many district's policies, potentially expose access to the teacher's personnel data, and provide access to information beyond what would be required by the substitute's legitimate interest".

Ethics and Norms

In each situation outlined, administrators should consider the difference between the legal ability to disclose student health information in particular situations and the ethical rightness of doing so. Sometimes, legality and ethics overlap perfectly (as in the case in Situation 3); in Situation 3, it was not only legal to disclose information about Jimmy's autism and nonverbal condition to law enforcement in an emergency situation (albeit in a way that preventing disclosure to others was unavoidable), but it was ethical in that doing so may well have mitigated harm. Sometimes, the line is fuzzy, as in Situation 2; However, the teacher might have the legal right to very broadly disclose information school-wide, depending on the school's definition of "legitimate educational interest," there may have been a better way to make sure that expectations were aligned by having the 504 team raise this possibility with Jack's mother.

School leaders must also ensure that they release student health information only when necessary because releasing personally identifiable health information creates or amplifies the risk for the students whose information is released and potentially for the district. The release of such data (e.g., through unsecured email, in case a binder of information is left in the wrong place or via careless talk in the lounge or the stands at an athletic event that unauthorized persons can overhear) can be harmful. Errant release of health-related information could subject the student to teasing or unwarranted harassment. These harms may not be preventable, but educators can mitigate them with empathetic, thoughtful communication and data privacy practices.

In another example, Situation 4 involved issues with food allergens and a seizure disorder at the secondary level; while the manner of sharing information with the long-term substitute was appropriate as described, leaders should consider how such information will be shared with other substitutes (long and short-term) when they arrive on campus and how to share such information in ways that benefit students without compromising privacy. At the elementary level, snack calendars are sometimes used to reduce burdens on families; families provide a snack for the whole class rotating to ensure all students have a snack. In this instance, general allergen

information would need to be shared (e.g., “no nut- or nut-products may be provided”) but in no case should individual students’ names be attached to communication: It’s simply not necessary to identify students and their particular allergens to safeguard health and wellbeing when communicating class-wide restrictions to families outside of the classroom.

Leadership Practices & Data Use

As challenging as it may be, school leaders must develop and maintain awareness of many issues that affect a school simultaneously, and often these intersect with the duty to create and sustain a safe campus environment. Sometimes student data privacy slips to the bottom of the list of pressing concerns, as leaders can mistakenly assume that procedures in place are being followed and that all school personnel are working within policies and procedures from a common knowledge base and with fidelity. At the same time, student safety often intersects with issues of data privacy, so leaders should remember (and communicate to others) that the two are not separate issues: Data privacy practices (when or when not to share health-related information and with whom to share such information) falls at the intersection of privacy and safety goals.

Leaders may be lulled into believing that procedures related to data privacy, as they apply to student health and well-being, are well-understood by all persons on campus. However, as with any human-dense system and thus “socially complex” (Fullan, 2016, p. 67), understandings may vary, and practices may be inconsistent. This is especially true in schools with frequent turnover or substitutes–when the adults in the building change frequently, knowledge and clear understandings about privacy practices and what to do to protect student health and wellbeing can be lost. Therefore, it is incumbent on leaders to ensure that all personnel has proper training (and retraining, as policies and laws evolve, and onboarding, as new personnel joins the team and others exit the system) and to establish and monitor systems that guide and track access to student education records.

Leaders also need to lean into frequent and transparent communication strategies, both to build trust with school personnel, families, and communities (e.g., Tschannen-Moran, 2014) and to empower teachers to ask questions when they are unsure about potential releases of information and act decisively in sharing in emergency situations. Trust, communication, and caring affect the ability of principals to effectively lead schools (Grissom et al., 2021, p. 56); leaders therefore need to be intentional about how they act to engender open communication, trust, and caring. One way to do this is to be clear and consistent about how school personnel act in concert to protect students while also acting professionally to protect and honor student privacy.

Leaders must address potential privacy violations as they occur, but it’s also incumbent on them to do due diligence to prevent such occurrences in the first place. This means educating staff on what comprises educational records, when HIPAA does and does not apply (in public schools, it almost never applies to student data), and when, under what conditions, and with whom sensitive student information/educational records may be shared.

References and Resources

Some school health requirements, such as required/recommended vaccination schedules and exemption requirements, vary by state, it's important to consult your local and state education agency's websites for specific or updated guidance; the resources noted below are a good starting place.

- Center for Disease Control. (n.d.). *School vaccination requirements and exemptions*. Retrieved from https://www.cdc.gov/vaccines/imz-managers/coverage/schoolvaxview/requirements/index.html
- Fullan, M. (2016). *The new meaning of educational change* (5th edition). Teachers College Press.
- Future of Privacy Forum (2021, October 5) *Student privacy primer.* https://studentprivacycompass.org/resource/student-privacy-primer/
- Grissom, J.A., Egalite, A.J., & Lindsay, C.A. (2021). *How principals affect students and schools: A systematic synthesis of two decades of research.* The Wallace foundation. Available at https://www.wallacefoundation.org/knowledge-center/pages/how-principals-affect-students-and-schools-a-systematic-synthesis-of-two-decades-of-research.aspx
- Hedden, E.M., Jessop, A.B., & Field, R.I. (2014). An education in contrast: State-by-state assessment of school immunization records requirements. *American Journal of Public Health 104*(10), 1993-2001. https://doi.org/10.2105/AJPH.2014.302078
- Tschannen-Moran, M. (2014). *Trust matters: Leadership for successful schools* (The Leadership & Learning Center). Jossey-Bass.
- U. S. Department of Health and Human Services [DHHS] and U. S Department of Education [ED] (2019). *Joint guidance on the application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to student health records.* https://studentprivacy.ed.gov/sites/default/files/resource_document/file/2019%20HIPAA%20FERPA%20Joint%20Guidance%20508.pdf

Facilitator's Guide: Student Health Information

Teaching Notes and Considerations for Scenario Facilitators:

In this scenario, leaders must consider the need to protect student data – their personally identifiable information, particularly regarding health and wellness. Leaders must also parse differences in protecting educational records, per FERPA and protecting "medical records" as stipulated/directed by HIPAA. Leaders need to understand which laws and policies affect schools, and they must deal legally and ethically with health-related data and information– information that, if shared, can risk student privacy and safety, and if not shared (appropriately), can risk student health, wellbeing, and even lives. Leaders must not only engage with health-related data in ethical and legally permissible ways, but they are also responsible for ensuring that personnel they supervise (at the campus or district level) safeguard and use student health data responsibly.

Extending Activities

- Compare and contrast FERPA and HIPAA. Who/what entities are subject to each, and in what ways? [See DHHS & ED, 2019, in references below for assistance.]
- Explore where student health data are stored in your district/school. What is kept in physical cumulative folders? What is maintained in a nurse's office, or other secure location? What is maintained in an electronic database or student information system? What is stored in classrooms, or in systems accessible by teachers in classrooms? What are the procedures for gaining access to student data via any of these locations (physical or electronic) and who has the authority to access it?
- In many elementary and primary schools, students receive most if not all of their core instruction in a homeroom class (or perhaps rotate among a small, departmentalized team). "Daily snack" is a common ritual, and while some schools have students bring their own snacks, others use a snack calendar, rotating the responsibility through families. Rotations can help ensure a bit more equity in terms of the types of snacks offered and mitigate the risk of a student either not having a snack (in which case school personnel and services often step in to provide needed food) or of being singled out for having snacks considered subpar by peers. Consider snack time in light of food allergies and other potential medical issues. Dialogue about appropriate ways of informing substitutes and classroom volunteers about student-specific allergies:
    - When and under what conditions can or should student-specific information be shared (and with whom)? When should sharing such information be only in general, non-identifying ways?
- Brainstorm the kinds of harms that may accrue to students if health information from their education records is intentionally or inadvertently released to unauthorized persons.
- Working from district policies, develop a brief training to help teachers understand when and under what conditions they can share student-specific health information, such as allergies, with other school personnel (e.g., substitutes, custodians, colleagues/club sponsors) or non-school personnel (e.g. law enforcement, classroom volunteers). Is this

different from any other type of education record information? If no such policy exists in your district, collaborate around a draft policy proposal that keeps children safe while also aligning with student privacy laws.

De-Identified and Aggregate Student Data

Learning Objectives

- Understand what it means for data to be properly de-identified including awareness of techniques for de-identification.
- Understand what it means for data to be properly aggregated.
- Differentiate between using de-identified and aggregate data and generate examples where each would be the most appropriate.
- Identify circumstances where, even with certain variables (e.g., first name, last name, age, grade) being withheld, people may still be able to identify students based on existing characteristics.

The Maximilian School District is a small but growing district with three elementary schools, one middle school, and one high school. Elementary principals have been asked to present "data-based improvement and action briefs" at the upcoming Board of Education meeting. The goal of the presentations is to demonstrate trends in achievement, campus climate, and student behavior. This data will guide a discussion on the leadership team's planned next steps. Similarly, district-level program directors were asked to provide programmatic data demonstrating the program's impact on student achievement, growth, and development. In preparation for the meeting, district leaders met to run through their presentations.

- Ms. Luna talked about reducing disciplinary infractions and a slow but positive trajectory in mathematics scores for students at Armstrong Elementary. She showed a snapshot of a teacher's screen in the new assessment system. The snapshot demonstrated how teachers (and administrators) can see the student's name, class period, birthdate, special program indicators, race/ethnicity, class-level grades, and prior benchmark assessment and state assessment scores. She had blacked out student names, though the screenshot retained a grade-level marker in the upper right corner (4th grade) and the teacher's first initial-last name in the lower left (M. Holbrook).
- Mr. Cooke, principal of Dawson Elementary, took a similar approach, though he presented aggregate trends with screenshots from the assessment system training and a tool Dawson's leadership team used to track disciplinary infractions and interventions. He presented the data by grade band (Kindergarten through 2nd grade, 3rd through 5th grade), with teachers' and students' names removed. He also showed trends within these bands by special program markers, gender, and race/ethnicity as used by the state accountability system.
- Dr. Hansen, the director of special education, focused on the department's efforts to close gaps in performance between students who qualified for special education services and students who did not qualify. As she was to follow the other presentations, she spoke to Armstrong and Dawson Elementary Schools' practices related to communication. To illustrate, she shared two slides highlighting closing gaps for students receiving special education services at several campuses. No individual student names or IDs were included. However, two reports, academic performance, and disciplinary incidents were

presented in a matrix form that included gender and race/ethnicity, this data was presented by grade band (K-2 and 3-6). Due to the smaller enrollments in these two elementary buildings, some bands had fewer than 10 students receiving special education services.

- The district McKinney-Vento coordinator, Mrs. Falcon, presented geographic data on the district's contracted private transportation services. Private transportation is provided to students who qualify as homeless under McKinney-Vento and reside outside of the district's normal transportation zones. Many students are transported from outside of the district boundaries. The data is aggregated by neighborhood/zone, school attended, and grade. In hopes of showing the need for continued private transportation, in spite of the significant cost, she draws correlations between the frequency of ridership, a decrease in disciplinary incidents, and an increase in student performance.

After the planning meeting, the principals and directors were chatting. As the chat progressed, Ms. Luna admitted she was a little chagrined to notice she hadn't removed grade level or teacher names from her slides as there are only two children of Asian ethnicity in that classroom, a boy and a girl. They then began to review all their slides to determine if any other data could lead to the identification of individual students.

Discussion Questions

- What–if anything–should each of the presenters have done to protect student privacy better and mitigate the changes that the reports could be compared to re-identify students? Consider the combination of different data sets presented by all administrators.
- If the standard is that PII includes "other information that, alone or in combination, is linked or linkable to a specific student that would allow a *reasonable person in the school community, who does not have knowledge of the relevant circumstances, to identify the student with reasonable certainty*" (Leichty & Leong, 2015, p. 2, emphasis added), which presentations, if any, could be a violation of FERPA?
- How would the risk of re-identification be mitigated in a larger district? What are the implications for a small district?
- If you were the principal or program director, how would you have accomplished the task while protecting privacy? In what other venues would de-identification be appropriate and required?
- Under what circumstances, and with whom, would you as a school or district leader, use individual student-level data? Under what circumstances, and with whom, would you, as a school or district leader, use aggregate data?
- What subgroups exist within your school that include too few students to properly de-identify or aggregate data? How might you present data without exposing the students?

From the Evidence Vault:

- Flanagan, B., & Ogata, H. (2017). Integration of learning analytics research and production

systems while protecting privacy. *Proceedings of the 25th International Conference on Computers in Education,* 1-6. https://www.researchgate.net/profile/Brendan-Flanagan-2/publication/321717317_Integration_of_Learning_Analytics_Research_and_Production_Systems_While_Protecting_Privacy/links/5bad71c845851574f7ebd063/Integration-of-Learning-Analytics-Research-and-Production-Systems-While-Protecting-Privacy.pdf

- Klose, M., Desai, V., Song, Y., & Gehringer, E. (2020). EDM and privacy: Ethics and legalities of data collection, usage, and storage. (ED607820). ERIC. https://files.eric.ed.gov/fulltext/ED607820.pdf

In the News / In the World of Practice:

- Arbuckle, L. (n.d.). Aggregate data provides a false sense of security. *Privacy Tech*. https://iapp.org/news/a/aggregated-data-provides-a-false-sense-of-security/
- Herold, B., & Davis, M. R. (2015, Aug.). 'De-identifying' student data is key for protecting privacy. *Education Week*. https://www.edweek.org/technology/de-identifying-student-data-is-key-for-protecting-privacy/2015/08
- Kochovski, A. (2023, April 25). What is data anonymization & de-identification in 2023: Is it truly anonymous? *Cloudwards.* https://www.cloudwards.net/what-is-data-anonymization/
- Polonetsky, J. (2015, Feb.). Data de-identification: Useful tool, but no magic bullet. *EdSurge.* https://www.edsurge.com/news/2015-02-10-data-de-identification-useful-tool-but-no-magic-bullet
- Schneier, B. (2007, Dec.). Why 'anonymous' data sometimes isn't. *Wired*. https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/
- Votipka, J. (2023, April 10). ACLU expresses privacy concerns after documents from Northwest in Grand Island reveal identifying information. *Lincoln Journal Star.* https://journalstar.com/news/local/education/aclu-expresses-privacy-concerns-after-documents-from-northwest-in-grand-island-reveal-identifying-information/article_c984ef81-1d2c-599d-b708-7713dc0bb66e.html

Data Privacy and Compliance Considerations

Data de-identification has been defined by the U.S. Department of Education's Privacy and Technical Assistance Center as "the process of removing or obscuring any personally identifiable information from student records in a way that minimizes the risk of unintended disclosure of the identity of individuals and information about them" (2013, pp. 2-3). An important point in understanding anonymized data is that data may be "de-identified" in such a way that a particular data set lacks links to personally identifiable information, but may, if not de-identified in concert with other, related documents, not be "anonymized." That is, it's often possible for persons to use more than one data set to piece back together data in such a way that data become "re-identified" (Educause, 2015). Total anonymization may not be desirable, as data linkages often enable worthwhile evaluation and research efforts that benefit systems and individual students. However, appropriate, and thorough de-identification techniques need to be used to minimize the odds of inadvertent and inappropriate releases of data.

As an example of de-identification that may lead to unintended disclosure of individual information, consider an elementary school in a small school district. Prior to the start of the year, the principal posts class rosters by grade level and homeroom teacher; the rosters include students' first and last names. Later in the year, a report is given at a meeting in which data is shared that breaks down benchmark data by the final three digits of student ID numbers and student sex, race, and grade levels. A document related to a field trip lists homeroom teachers by grade level and students' first and last names. A handout used in a faculty meeting and emailed to staff lists benchmark data and includes teacher names, student ID numbers, and markers for student race and at-risk status. A report for the school board uses grade level, the last three numbers of the student ID, and a code that conveys which special education services (if any) a student qualifies.

Especially if a school does not have numerous sections of a class or a range of diversity within and across classes and grade levels, one can see how simple it might be to combine these documents and "backward map" names to ID and to use names, ID, grade level, special services codes, student sex, race, and homeroom teacher to discern the identity of individual students. For this example, we will imagine that a Hispanic boy in 2nd grade in Mrs. Foster's class with the last three ID numbers of 789 qualifies for speech services under "Other Health Impairment."

No one clue is forthright, but taken in aggregate, these facts provide ample information about this individual student.

Provided that Mrs. Foster's class has only one boy identified as Hispanic, the data have been "re-aggregated" in a way that reveals protected information. This may be an extreme example, but in small school settings, it is possible for subgroups of students to be so small in sample size that individuals are identifiable through the combination of publicly available data. This is why following district data protocols and funneling requests for data through a data handler/processor who understands which documents redact, remove, or otherwise mask particular data to protect against re-identification is important. Proper data de-identification requires "deep technical knowledge and expertise and adherence to industry best practice. Therefore, student data holders should not attempt to de-identify student data sets without competent support (Leichty & Leong, 2015, p. 8). Data processors or handlers know which protocols to follow with consistency to mitigate the likelihood of reports that present the opportunity of re-aggregation from being released. For example, they may report only by grade level or by teacher code when preparing data sets for public consumption or researchers. If leaders are asked to present data-based reports, they should also be trained to format data for these reports so they do not inadvertently present data sets that allow for re-identification.

In part, because Maximilian is a relatively small school district, the removal of only last names is insufficient in terms of de-identifying individual students. An individual who knows the district and the students might easily be able to extrapolate across presentations or even within a presentation to identify specific students based on their characteristics, such as being in special education or qualifying for transportation under McKinney-Vento. Even if the district were larger, only removing students' last names is an ineffective and insufficient de-identification strategy that does not adequately protect the privacy and confidentiality of the students. Extreme care must be taken when presenting authentic student data.

Data de-identification "begins with eliminating all direct student identifiers from an educational record, but education agencies and institutions, and other data holders, must take further steps to ensure that indirect identifiers or other information do not enable an unauthorized actor from determining a student's identity" (Leichty & Leong, 2015, p. 2). Some of these approaches include:

- Blurring: Reducing the precision of disclosed data to minimize the certainty of individual identification. For example, converting continuous data elements into categorical elements that subsume unique cases.
- Perturbation: Making small changes to the data to prevent the identification of individuals from unique or rare population groups. For example, swapping data among individual cells introduces uncertainty.
- Suppression: Removing data, for example, from a cell or row, to prevent identifying individuals in small groups or those with unique characteristics. (Leichty & Leong, 2015, p. 3)

Of course, some approaches used to mask identifying information are simply ineffective. For example, using the black highlighting tool to "excise" names in Word or a .pdf can reveal the sensitive data just by copying the text and pasting it into a new document." Using a black marker to black out names often still leaves names legible, particularly if simply blacking out on an original or on a first-run copy (that is, this may be effective if the information is blacked out, then run through a copier, and then repeated until illegible; of course, at that point, there are also several copies of the private data being generated at the copier, and proper disposal requirements come into play). A better approach is to use redaction features specifically built for the purpose, such as the redaction tool in Adobe Acrobat Pro, or any tool that offers this feature. One strategy that *can* be used with care is to substitute students' real names, and other identifiers, with fictitious names or randomized codes, or other pseudonyms. Such replacement must be mindful of not substituting with names that reflect gender or ethnicity which could also be a means to identify the students. If later reidentification is necessary, keys intended for use in re-identification should be kept separate from the masked documents. In the case of inadvertent disclosure, the likelihood of matching codes or fictitious names to actual students is reduced. According to the *Forum Guide to Data Privacy* (2016), "the goal is for a reasonable person not to be able to identify an individual student based on the data shown" (p. 24).

Ethics and Norms

A fundamental principle of appropriate and ethical data use is for educators to understand the importance of protecting the privacy of personally identifiable information. When educators use authentic student data, the identifiers must be removed or appropriately hidden so that no one can identify a particular student or group of students based on the data and personal characteristics or variables. Careful de-identification is needed. Educators might tap resources such as the Forum Guides on Data Privacy and Data Ethics to provide guidance on how to navigate policies around responsible data use and how to protect the privacy and confidentiality of student data in presentations or in any sort of conversation.

Leadership Practices & Data Use

Leaders should be mindful of how they and their staff present when authentic student data are included. They should consult district policies and ask district data processors/handlers what protocols should be followed when preparing data reports that need de-identification. In turn, they should provide training for their staff about how to make presentations that ensure the protection of student privacy and confidentiality. Leaders should standardize procedures and policies in their schools and districts, laying out accepted de-identification strategies. They must make clear that simply removing students' last names does not ensure sufficient protection. Resources are available from various agencies that can help local education agencies set policies and provide guidance to practitioners about how to make presentations responsibly without risking the identification of individual students.

EDUCAUSE (2015) suggests five questions to consider when addressing requests for de-identified data, and it would benefit school leaders to use these as a guide for mitigating risks of privacy violations when dealing with data de-identification and releases (including public records requests):

1. To whom should a request for a de-identified data set be made?
2. Who works with the requestor to understand the request, analyze the data, and identify what data elements must be de-identified?
3. From whom must approvals be obtained before the design/proposal to provide de-identified data is accepted?
4. If there is a cost either in resources or budget to do the work, who approves the cost estimates? Who pays?
5. Is it acceptable for a data steward or other members of the approval team to refuse the requests on grounds other than confidentiality?
6. What technical resources are available to do the de-identification?
7. Document the provision of the de-identified data to the requestor.

In addition, in scenarios like the one highlighted in this case, where school principals and district department leads are asked to present data in a public forum, several of the above may not apply, as there is not technically a "request" for de-identified data. However, a useful parallel process would be to have those persons submit their planned presentations to a data steward/handler for review so that someone more "in the know" on what other reports have been released, and in what formats, that could potentially compromise privacy due to the possibility of aggregation and re-identification, can help avoid unintentional breaches. A benefit of such a process is that the data steward may also notice de-identification errors within the system and foreground these in training for school-level leaders and district-level leads so that over time fewer such errors are made.

References and Resources

- Educause. (2015, Jul.). *Guidelines for data de-identification or anonymization*. https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-

program/resources/information-security-guide/toolkits/guidelines-for-data-deidentification-or-anonymization

- Finch, K. (2016, Apr.). *A visual guide to practical data de-identification*. Future of Privacy Forum. https://fpf.org/blog/a-visual-guide-to-practical-data-de-identification/
- Leichty, R. & Leong, B. (2015, August). *De-identification & student data.* Future of Privacy Forum. https://fpf.org/wp-content/uploads/2021/05/FPF-DeID-FINAL-7242015jp.pdf
- Leong, B. (2015, Aug.). *Student data and de-identification*. Future of Privacy Forum. https://fpf.org/blog/student-data-and-de-identification/
- National Forum on Education Statistics. (2010). *Forum guide to data ethics* (NFES 2010-801). U.S Department of Education, National Center for Education Statistics. https://nces.ed.gov/pubs2010/2010801.pdf
- National Forum on Education Statistics. (2016). *Forum guide to education data privacy*. (NFES 2016-096). U.S. Department of Education, National Center for Education Statistics. https://nces.ed.gov/pubs2016/NFES2016096.pdf
- Office of the State Superintendent of Education. (n.d.). *Student privacy and data suppression policy at a glance*. District of Columbia Public Schools. https://osse.dc.gov/page/student-privacy-and-data-suppression-policy-glance
- Privacy Technical Assistance Center (2013, May). *Data de-identification: An overview of basic terms.* U.S. Department of Education. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/data_deidentification_terms.pdf

Facilitator's Guide: De-Identified and Aggregate Student Data

Teaching Notes and Considerations for Scenario Facilitators:

Scenario users will encounter and explore multiple applications of data privacy, data ethics, and leadership as they read, work through discussion questions, and engage in the suggested activities. While not all applications of data use and data sharing, ethics, and privacy will be covered by these teaching notes, below we point out several areas that facilitators may choose to emphasize as they lead groups in learning with the "Anonymized Student Data" scenario.

Extending Activities

- Place yourself in the role of the MSD Superintendent. Develop a checklist or guidelines for those principals and program directors to use as they present data, to decrease risks of inadvertent release of PII, either within a single presentation or through the combination of various presentations.
- Discuss the pros and cons of using aggregate vs. de-identified student data vs. anonymized student data. Generate some examples where each would be needed and appropriate, and then discuss what steps must be taken in each of those examples to ensure the appropriate procedures are applied to result in the kinds of data to be used.

Balancing Parental Pressure and Student Privacy

Learning Objectives

- Explain what data or information can be shared with particular persons/audiences, and what kinds of student information may only be discussed or shared with particular persons pursuant to FERPA.
- Develop and practice approaches for setting meetings/conference norms so that school leaders can engage with parents, family members, or legal guardians of students in FERPA-compliant and ethical ways.
- Identify appropriate ways to group and regroup students for instruction that protect student privacy.

Mr. Dusty is the principal of Cochran Middle School. CMS serves just over 800 students and is in a generally affluent community. Historically parents have exercised their voice in effective ways in order to influence their children's education. Recently, parents at CMS want updated and complete access to all of their children's data through the school data portal.

One morning, Mr. Dusty arrives at the office only to see three parents, waiting for him in the main office. One of the parents, Mrs. Piper–the current PTA president–smiles and greets Mr. Dusty before looking at him more seriously: "Mr. Dusty, we have a pretty important concern we really need to talk to you about. I'm sorry we didn't make an appointment–it was only last night that we were talking and realized what was happening. Mr. Johnson wanted to call the superintendent's office, but I suggested we talk with you first to see what can be done."

Assuming the issue was a problem with the fast-approaching school carnival and that it could be resolved fairly easily, Mr. Dusty nodded before inviting the parents into the conference room. "I have a few classroom visits scheduled, but they are brief walkthroughs, so I can push them to this afternoon or tomorrow morning. Come in and tell me what's going on."

The group settled around the conference table, and from the opening salvo, Mr. Dusty knew he'd made an error in his assumption of the topic at hand. Mrs. Piper explained that the math department had begun using biweekly computer-based assessments to group and regroup students for reteaching. Students who mastered the standards being assessed were engaged in "Challenge Activities" during homeroom time, while students who needed reteaching worked with the math teachers in activities related to concepts they hadn't mastered.

Mr. Dusty was well aware of the practice; the entire campus talked about ways to use the homeroom period better and had started using it for flexible grouping the prior semester. All students had a choice of activities on Tuesday and Thursday, and on other school days students were directed to leveled groups in reading and/or mathematics. This helped match students with needed reteach by content area and learning objective. He was also aware that one of the reasons the district selected these computer-based assessments was that the program had the ability to generate suggested groups around both standards-based strengths and weaknesses. This allowed for a quick turnaround between assessment and instructional response. He'd talked

about the flex grouping and assessments in his campus communications, so he was puzzled at why this concern was presenting itself now.

The second parent, Mr. Johnson, further explained. “Of course, the kids hate it because they miss out on one of the few times of day they used to get some free time or visit with friends in their homeroom. But a bigger issue is that the groups seem inaccurate. My son, Jim, is in GT and hasn’t been in a Challenge Activity group yet, so he sees kids doing robotics and engineering activities and never gets to do any of those fun activities that involve higher-level math. Yet there are two students–Ginny and Manny, I think–who Jim says literally go to the learning lab for support regularly, so I assume they are in special ed, and they’ve both been in the top groups three times. How is that even possible? Jim even said Manny was retained last year, so I find it hard to believe he is knocking the top off his math tests, even with whatever special ed help he has.”

The other parent nodded, before Mrs. Piper added, “I’m not saying Robby should always be in the top group, even though he’s GT too–we know that sometimes he doesn’t do his best work and of course he has some test anxiety. But he’s been in the bottom group twice already, and everyone in the class treats him like he’s dumb now! If GT kids are never in the Challenge groups, how accurate can these assessments be? We really want the teachers to stop calling the students out like this and get back to teaching how they did before all this grouping. As soon as the groups get posted, everyone knows who did great and who didn’t on the last exam, and the kids in the bottom groups get made fun of. That’s not right, even if the system is set up to help them learn.”

Mrs. Knight, the third parent, jumped in. “Also, I talked with parents from last year, and evidently the teachers our kids have–Ms. Lydia and Mr. Mac–had issues all last year. Neither has been teaching long, but parents said their classrooms were chaotic and Mr. Mac was on a growth plan! If they don’t know what they’re doing, I’m worried about how Susan will do next year in Algebra. It’s at the point I may have to pull her and enroll her at Fieldstone Academy mid-year, which I didn't want to have to do, but if she has a bad year in math, it will ripple out to not just 8th grade but also her whole high school math course sequence.”

Mr. Dusty barely had time to collect his thoughts–he’d been expecting a fairly minor issue related to the carnival, not a barrage of academic progress and teacher-quality questions. Discombobulated, Mr. Dusty began to talk about Ms. Lydia’s and Mr. Mac’s successes in the previous year on the state exam.

When Mrs. Knight pressed on issues of classroom management and asked about Mr. Mac’s “growth plan” from the previous year, Mr. Dusty managed a fairly lame, “I can’t discuss employment issues with you,” realizing that this probably only threw fuel on the fire, even though Mr. Mac was decidedly not on a “growth plan” in the previous year. “I’d be happy to set up conferences for each of you with your child’s teacher and Mr. Rex, the math department chair, to review assessment data and your child’s progress, but can’t discuss employment matters or other children with you–I hope you understand–just like I would never discuss your children or their progress with other parents.”

"But that's part of the problem," Mrs. Piper continued. "You don't have to, because we all know how everyone's children are doing because of what group they are in! And the other kids know too. And part of our concern is that the assessments aren't accurate, so how do we get a more accurate test so we know whose kids need what and that they get what they need?"

After about a half hour of back and forth, Mr. Dusty asks if he can have a few days to collect more information from Ms. Lydia and Mr. Mac, as well as from the math department chair, and then follow up with the parents. They agree though he has no confidence that the time will dissuade them from calling the district immediately. As they leave, Mr. Dusty has a gnawing sense that not only does he need to problem-solve around the concerns noted, but that he should have guided the discussion with the parents in a more constructive way.

Discussion Questions

- What are the implications if Mr. Dusty or Mr. Rex use student data and mention specific students, given that the parents are present? Is it acceptable for them to talk about Jim, Susan, and Robby since all of their parents are present and were the ones who initiated the conversation? Why or why not?
- Would mentioning other students' performance make a difference if the discussion was one-on-one with a specific student's parents, rather than the group meeting?
- What are the implications if the parents were the ones who discussed the student data rather than the administrators?
- If Mr. Mac was not on a growth plan the previous year, would it have been acceptable for Mr. Dusty to correct the parent? Why or why not?
- In this scenario, the teachers post groups of students so students know where to go during homeroom for their flex groups. If there is no assessment data posted (i.e., only names of students and classroom/teacher assignments during homeroom), has student privacy been violated? What should this process look like to facilitate both efficiency and protect privacy?
- How could Mr. Dusty have avoided or diffused the situation more effectively?

From the Evidence Vault:

- Calarco, J. M. (2020). Avoiding us versus them: How schools' dependence on privileged 'helicopter' parents influences enforcement of rules. *American Sociological Review 85*(2), 223-246. https://doi.org/10.1177%2F0003122420905793
- Calarco, J. M. (2020). When 'helicopters' go to school: Who gets rescued and who gets left behind? [Briefing paper prepared for the Council on Contemporary Families]. https://sites.utexas.edu/contemporaryfamilies/2020/03/01/when-helicopters-go-to-school/
- Tschannen-Moran, M. (2014) The interconnectivity of trust in schools. In D. Van Meale, P. B. Forsythe, and M. Van Houtte (Eds) *Trust and school life: The role of trust for learning, teaching, leading, and bridging* (pp. 57-81). Springer.

In the News / In the World of Practice:

- Feirsen, R., & Weitzman, S. (2021, April 1). Constructive conflict. *Educational Leadership 78*(7). https://www.ascd.org/el/articles/constructive-conflict

Data Privacy and Compliance Considerations

Parents can converse about their children with school personnel, and they have the right to talk with other parents about their children (on or off school premises); what is prohibited is school personnel talking to parents in ways that reveal data or PII about other people's children, (see Myers, 2017). While there may be limited circumstances where multiple families are all present in one meeting (for example, to participate in conflict resolution or a restorative exercise with consent from all parties and with a facilitator), the possibility exists of parents raising issues that involve their own and other people's children in public forums (e.g., town halls, campus meetings, PTA meetings, school board meetings). Leaders need to be prepared for others to breach privacy boundaries, and they need to be ready to respond in responsible, constructive ways.

To this end, leaders should never assume they can share student information or data with another child's parent, family member, etc. If a leader doubts what data can be shared and with whom, they should always check compliance requirements in local policy and seek advice from the district's legal counsel. Periodically reviewing local policy as well as broader guidance (such as Park et al., 2021 and the School Administrator Privacy Primer, both from the Future of Privacy Forum), can help leaders approach these situations with confidence. A good general guide is, when in doubt, only share student-specific information with that student's legal parent/guardian. Any sharing beyond that needs to be supported by appropriate consent documents or context-specific policies that permit sharing (e.g., emergency situations).

In the scenario presented, Mr. Dusty should confine himself to talking about the students mentioned only with their legal parent/guardian; it does not matter whether he is talking with parents individually or as a group. Of course, parents (at least those not employed by the school) are not beholden to FERPA; they can make assertions or talk about other children, even if it might be impolite or indiscreet. This is one of the administrative challenges; parents and students may be able to make statements in a group or public setting (at least to a degree), and educators are constrained as to how and in what context they may respond, but FERPA's privacy constraints attach to school personnel–not to the parents, students, or family members.

While FERPA deals with student PII, and the inquiry around teacher evaluations/growth plans does not fall under FERPA, the inquiry and statements likely fall under a district's human resources policies. It would have been appropriate for Mr. Dusty to simply say, "Of course, I cannot discuss personnel matters with parents, though that is certainly an employee's right to do so," and to offer broader observations about a class or to broker a conference with that teacher.

Ethics and Norms

Group meetings such as the one depicted in the scenario require sensitive and delicate treatment. They should also be accompanied by preplanning and, wherever possible, exploring

issues and facts beforehand. This can avoid surprises (as Mr. Dusty experienced), help leaders know when a group meeting would be inappropriate or invite privacy violations, and allow them time to reschedule individual meetings if needed. In any group setting, leaders must establish norms and expectations so that the meeting can be productive without violating anyone's privacy.

While this scenario deals with complaints about curriculum and instructional issues, school leaders may more frequently encounter issues like the "sudden group parent meeting request" when an issue pertains to discipline or bullying. In fact, one area of student privacy considerations in recent years has involved what video evidence may be viewed by parents when a video (of a bus or cafeteria incident, for example) involves children other than their own. Some rulings have held parents can view these, under certain conditions, while others have required that consent of parents of all children present be obtained before showing such evidence to parents (Myers, 2017).

This particular scenario also deals with the leader's role in mitigating potential harms to the school and to teachers. As documents related to teacher evaluations/performance are confidential, Mr. Dusty is in a predicament not unfamiliar to experienced educators. The parents are free to allege that "Mr. Mac was on a growth plan"; however, Mr. Dusty is bound by professional ethics to offer no response. This dynamic often (and frustratingly) plays out in the media, where dissatisfied parents are free to present their side of an issue to a reporter, while school personnel must be more guarded in responses. This can seem like a no-win situation, as leaders may never feel they can "get the whole story out."

Even though it was the parents who initiated the discussion of student data (and discussions of teacher evaluations) in a group setting, Mr. Dusty missed an opportunity to "hit pause" with a bit more resolve. Mr. Dusty would have been well within his role to state, "We've begun wading into discussions that involve multiple children, and children whose parents aren't present, so I need us to take a brief time out. I am ethically and legally bound only to discuss student information and data with their parents or legal guardians. You all can, of course, discuss these things outside of the school however you like, but in my role here, I have some additional responsibilities. Just as I would never discuss any of your children with other parents, I can't engage in a conversation that involves sharing information about other people's children–and that includes those children's performance, program status, etc. I hope you understand that this is a boundary I can't cross because I respect your rights as parents. So we can limit the discussion to these more general issues, we can reconvene and I can talk with each of you individually, or we can agree not to bring other people's children into the conversation." However he wanted to do it, he should have made it known immediately that discussing other people's children in any way was inappropriate and would warrant ending the meeting.

Finally, one complaint raised by the parents was the posting of groups, and the inferences drawn by students about the abilities of students in those groups. If the flexible groupings are posted only with student names and destinations (i.e., supervising teacher and location), then there is no FERPA violation. If what is being posted comes directly from the computer-based assessment program and has any kind of assessment scores, color coding, or other markings that denote achievement, then the postings are in violation of FERPA. The school can further mitigate

potential violations by ensuring, for example, that the same teacher does not always have a group of underperforming students and that other teachers do not always have those who mastered the assessed objectives. Another approach to make this process more palatable is to ensure that all groups–whether accelerated or remedial–incorporate active, engaging opportunities to learn and adequately track student progress so that results can be demonstrated to parents/guardians, particularly those who doubt the usefulness of the flex grouping approach to meeting their child's needs.

Leadership Practices & Data Use

Leaders must respect their stakeholders/parents and listen carefully to their concerns. Yet, they also must take care not to buckle under pressure to share information that should be confidential. Leaders can take control of situations like the one presented in this scenario in constructive ways.

First, leaders can be proactive by obtaining a clear understanding of the situation before engaging in a group meeting and prior to making any major decisions. Taking some time–however brief–to do some questioning and fact findings prior to meetings can also help leaders know when they need to run a scenario by a mentor or district leader/district legal counsel. This can also buy time to work up a script to help shape the flow of the meeting and to practice norm/expectation setting; this can set the meeting up to be more about understanding and improvement than venting or complaining.

Second, leaders should listen to understand the concerns at hand and encourage concerned parties to follow established procedures in problem-solving; this often means directing (or assisting) parents in setting up an initial meeting with the person(s) closest to the issue. In this scenario, that would be the teacher-of-record for each student in question. Given that two of the students are served in GT programs, a team meeting (AP, math teacher, math department chair, and GT teacher) might be a good approach, but being consistent in the expectation that parents and professionals work together prior to escalating a problem is important. For professionals (including leaders) who struggle with conflict, resources and suggestions for navigating conflict productively can be readily found in *Leadership on the Line* (Heifetz et al., 2009), *Crucial Conversations* (Grenny et al., 2022), and *Crucial Accountability* (Patterson et al., 2013).

Finally, Mr. Dusty assumed the problem was something that had to be addressed immediately, which triggered a wholesale rearrangement of his planned work for the morning, which had been focused on instruction. While Mr. Dusty likely wanted to demonstrate his accessibility and availability to parents, he also needs to be consistent in his prioritization of instruction. If principals upend their focused instructional work for every email, drop-in, or call, they will routinely exist in reactive–not proactive–mode. A brief discussion to identify the actual problem could have led to scheduling an appointment, fact-finding, or to a referral of the parents back to the teachers themselves. Scheduling an appointment later but with the necessary personnel involved would also permit teachers and school leaders to collect and organize data to be adequately prepared to engage in an open and informed conversation about the issues presented.

References and Resources

- Cheung, O., (2000). U.S. Department of Education. *Privacy Issues in Education Staff Records: Guidelines for Education Agencies* National Center for Education Statistics, https://nces.ed.gov/pubs2000/2000363.pdf
- Feirsen, R. & Weitzman, S. (2022). From conflict to collaboration: A school leader's guide to unleashing conflict's problem-solving behavior. Rowman & Littlefield.

- Grenny, J., Patterson, K., McMillan, R., Switzler, A., & Gregory, E. (2022). *Crucial conversations: Tools for talking when stakes are high* (3rd edition) McGraw Hill.
- Heifetz, R., Grashow, A., & Linsky, M. (2009). The practice of adaptive leadership: Tools and tactics for changing your organization and the world. Harvard Business Review Press.
- Myers, T. E. (2015). *Your top ten FERPA questions asked and (hopefully) answered.* Bracket & Ellis, P.C. https://utcle.org/conferences/SL15/get-asset-file/asset_id/34838
- Park, J., Cotto, J., Waller Curtis, A., Klein, C. Reddy, A., Siegl, J, Sollberger, A., Triplett, J. & Vance, A. (2021, January 12). *Student privacy communications toolkit: For schools & districts.* Future of Privacy Forum. https://studentprivacycompass.org/resource/student-privacy-communications-toolkit-for-schools-districts/
- Patterson, K., Granny, J., Maxfield, D., McMillan, R., & Switzler, A. (2013). Crucial accountability: Tools for resolving violated expectations, broken commitments, and bad behavior. McGraw Hill.
- Future of Privacy Forum (2021, October 5) *Student privacy primer.* https://studentprivacycompass.org/resource/student-privacy-primer/
- Tschannen-Moran, M. (2014). *Trust matters: Leadership for successful schools* (The Leadership & Learning Center). Jossey-Bass.
- Whitaker, T. & Fiore, D. J (2015). *Dealing with difficult parents.* Routledge.

Facilitator's Guide: Balancing Parental Pressure and Student Privacy

Teaching Notes and Considerations for Scenario Facilitators:

This case allows users to work through intersecting challenges: leaders are required to establish and maintain productive relationships with a range of parents (and thus engage in and work through conflict) and to ensure that student personally identifiable information (PII) is only shared in legal and ethical ways. Therefore, the leaders in this scenario are challenged by working through conflict while attempting to protect the privacy of student data in front of parents who are not related to the students.

Extending Activities

- Create some short "scripts" leaders can use to establish expectations or norms for what staff and student personal information can and cannot be shared or discussed in a group situation.
- "Rewind" this scenario to various points, roleplay how Mr. Dusty could/should have responded and discuss the implications for his response and potential consequences of his various responses. At the very least, rewind to the following points in the scenario:
    - Mr. Dusty first meets the parents in the main office, and they request the meeting.
    - Mr. Dusty opens the meeting around the conference table by listening to the parent's concerns.
    - The parents bring up other students (Gina and Manny) and their (assumed) special education status, prior academic performance, and needs.
    - The parents bring up the performance/skill of Ms. Lydia and Mr. Mac, including the assumption that Mr. Mac was on a growth plan.
    - Mr. Dusty closes the meeting by asking for more time to investigate the concerns.
- What if instead of a parent meeting, this topic had come up in a public forum, such as a school board meeting, campus town hall, or a PTA meeting? How should Mr. Dusty handle the situation?

Balancing Student Privacy and Academic Integrity

Learning Objectives

- Define “cheating” and “academic dishonesty” in alignment with current district/campus definitions, and outline how various technology platforms may enable or hinder efforts to engage in cheating or academic dishonesty.
- Explain the benefits, limitations, and risks (legal and ethical) of proctoring or plagiarism- and/or generative-text detection software or other academic-integrity-focused technology platforms.
- Explain the benefits, limitations, and risks (legal and ethical) of AI-enhanced tools used for accommodations and/or student work creation.
- Identify the kinds of data that can be appropriately acquired through proctoring or plagiarism- or generative-text detection software or other academic-integrity-focused technology platforms.

Rockhill School’s leadership team meets regularly to discuss school initiatives, culture, and staff concerns. This team comprises teacher leaders, select support staff, building administration, and district curriculum specialists. During the most recent meeting, the team discussed academic integrity and the concerns with and benefits of the latest release of AI tools that compose written works.

The following is a summary of the discussion.

- Social Studies department chair Richard Jacks: In a few of our department meetings, teachers have reported that student cheating has increased.
- English department chair Tara Dalton: The English team has had several incidents of student plagiarism this semester. Some of the plagiarism is due to the students not understanding proper citation, but a few instances included submitting materials copied from online sources. A few students also turned in assignments previously handed in by another student.
- District curriculum specialist Dr. Westover: Given that more students are taking dual credit courses and certification exams online, students must understand academic integrity. We must also ensure secure assessments. In the past, we’ve focused most efforts on state-required tests, but the need for test security is getting broader each year.
- Principal Dr. Abby: We should not only talk about what’s going wrong, but we also need to connect our response to learning. Cheating breaches the code of conduct; we must be proactive as we can’t discipline our way out of this problem. Are there ways we can help students learn to use emerging tools in support of their work, rather than simply treating this evolving tech as a villain?
- Jacks: Teachers feel that the consequences are important when students cheat, but it is challenging to stay on top of the strategies some students use. We’re a long way from cheat notes. They have their phones on them, do assignments at home where their

internet is not filtered by the school, paste from online sources, and now have AI tools like ChatGPT to write responses for them.

- Dalton: Without a way to lock down their browser, students can just look up the answers for the quizzes included with our course materials. It's hard to assess student knowledge versus what they can look up or copy from the internet or online textbook.

The team brainstormed strategies and tools to help identify and mitigate plagiarism and cheating:

- Academic integrity lessons within each discipline
- Teach students how to verify the content created by the AI tools.
    - Many of these tools don't cite the source
    - One day they will be as prevalent as the calculator
    - We can't just keep banning tools/resources
    - AI creation is even showing up in tools we already use for student accommodations, such as grammar software for students with dyslexia
- Tools to detect, intervene, or assign consequences for cheating
    - Plagiarism detection software that can compare the student's work against content on the internet and work turned in by other students. This could also be a useful teaching tool if we show students how to use it to improve their writing. Some aren't trying to cheat–they just don't cite or paraphrase well.
- Lockdown browser for online quizzes and tests
    - We have the ability to monitor student screens but locking students out of everything but an exam/quiz (or another task) would be helpful.
    - There is uncertainty around how some of the lockdown browser tools fit with students who have accommodations through 504 or special education programs.
- Online proctoring service for students taking make-up tests (missing due to school activities, illness, etc.)
    - The service requires a camera to remain on during the assessment.
        - There is concern about students off campus being required to keep their cameras on. You never know what you'll catch in the background, and many students do not have private study spaces.
        - Some automated services have been inconsistent and unreliable in how they read or respond to students of different skin tones.
    - The student should be able to sign in from anywhere with internet access.

- Some would rather have a testing center on site.

Discussion Questions

- What other privacy and/or ethics concerns might there be when considering academic integrity-focused technology or platforms?
- What privacy and/or ethics concerns should be considered when discussing implementing AI tools such as ChatGPT?
    - What data might these tools collect?
    - How might these tools be used in the classroom without violating a student's right to privacy?
    - How might these tools be used in instructional ways?
- What kinds of data must be collected for teachers and administrators to detect potential cheating? Which of these are personally identifiable? What strategies might educators use to mitigate the need for PII in such systems?
- Some platforms collect not only writing samples (e.g., plagiarism tools), but information such as keystrokes, eye movement, and body movements as well as indicators or potential cheating.
    - Are these valid indicators of cheating? Why or why not?
    - How might the collection of this information pose a privacy concern?
    - If data collected via an academic integrity-focused platform prompted you to investigate potential cheating based on one or more of the indicators noted above, what other factors might you consider as you investigate the issue?
- What might be the risks and benefits of using academic integrity-focused technology in your context?

From the Evidence Vault:

- Duncan, A. & Joyner, D. (2022). On the necessity (or lack thereof) of digital proctoring: Drawbacks, perceptions, and alternatives. *Journal of Computer Assisted Learning 38*(5), 1482-1496. https://doi.org/10.1111/jcal.12700
- Nigam, A., Pasricha, R., Singh, T., & Churi, P. (2021). A systematic review on AI-based proctoring systems: Past, present and figure. *Education and Information Technologies 26,* 6421-6445. https://doi.org/10.1007/s10639-021-10597-x
- Yoder-Himes, D.R.. Asif, A., Kinney, K., Brandt, T.J., Cecil, R.E., Himes, P.R., Cashon, C., Hopp, R.M.P. & Ross, E. (2022). Racial, skin tone, and sex disparities in automated proctoring software. *Frontiers in Education.* https://doi.org/10.3389/feduc.2022.881449
- Zeide, E. (2023). Big proctor: Online proctoring problems and how FERPA can promote student data due process. *Notre Dame Journal on Emerging Technologies 3*(1), 74-140.

In the News / In the World of Practice:

- Burrows, S. (2023, March 7). Three steps to prevent ChatGPT misuse. *Education Week.* https://www.edweek.org/technology/opinion-three-steps-to-prevent-chatgpt-misuse/2023/03
- Chin, M. (2020, April 29). Exam anxiety: How remote test-proctoring is creeping students out. *The Verge.* https://www.theverge.com/2020/4/29/21232777/examity-remote-test-proctoring-online-class-education
- Gordon, A. (2022, September 8). Scientists asked students to try to fool anti-cheating software. They did. *Vice.* https://www.vice.com/en/article/93aqg7/scientists-asked-students-to-try-to-fool-anti-cheating-software-they-did
- Hill, K. (2022, May 27). Accused of cheating by an algorithm, and a professor she had never met. *The New York Times.* https://www.nytimes.com/2022/05/27/technology/college-students-cheating-software-honorlock.html
- O'Brien, M. (2023, January 6). Explainer: What is ChatGPT and why are schools blocking it? *AP News.* https://apnews.com/article/what-is-chat-gpt-ac4967a4fb41fda31c4d27f015e32660
- Rose, J. (2022, August 25). Judge rules schools can't scan your bedroom with creepy proctoring apps. *Vice.* https://www.vice.com/en/article/qjkj3w/judge-rules-schools-cant-scan-your-bedroom-with-creepy-proctoring-apps

Data Privacy and Compliance Considerations

As is the case with any technology tool or platform, the first step in protecting data privacy and ensuring compliance is only to implement platforms, apps, or software that have been appropriately vetted through district technology personnel and for which agreements have been solidified to govern data collection, use, protection management, and storage. In this scenario, the brainstorming session should be followed by a collaboration with district technology personnel as a next-step. Another approach would have been to invite technology personnel to the initial discussion or to have asked them for ideas, as they often know what platforms are industry standard. In no case should an individual educator require the use of apps or platforms that have not gone through the appropriate vetting process or use an un-vetted app or platform themselves that requires the provision of student PII (see Future of Privacy Forum, 2021 and Park et al., 2021).

A challenge with implementing some tools–like lockdown browsers–may involve considerations of device ownership. If a school owns and issues laptops to students, then it is within the purview of the school to install such software. However, if students have to access exams on a learning management platform through a personal or shared computer, requiring students to install software could be problematic (and might even be impossible, if a student is accessing a computer at a public library). Various platforms might also have constraints (e.g., usable on laptops but not tablets, or challenges in Mac or PC contexts). Other challenges attach to other

kinds of “academic integrity” efforts. For example, A federal court recently ruled that a public university’s use of room-scanning technology during a remotely proctored exam violated a student’s Fourth Amendment right to privacy (Ogletree v. Cleveland State University, 2022).

Finally, educators should consider what kinds of data they require students to enter into the system, particularly if uploaded documents (like essays/term papers in a plagiarism detection tool) are stored in a repository. Having students use code numbers, rather than a full heading (name, class, section, etc.) can help mitigate the risk of unauthorized access to identifying information, though this does not ameliorate the ethical problem of requiring students to, in effect, contribute their own work, without remuneration, to a plagiarism detection source bank, if that is required by the website’s terms of service. In any event, a primary concern from a data privacy and compliance perspective is having a clear understanding of what data are captured by the platform, whether they constitute PII, and what will be done with data (if anything) beyond school or district use (e.g., Barnes, 2015).

Ethics and Norms

Any time schools implement technology-based academic integrity tools, educators should consider issues of privacy and of “dataveillance,” or the use of technology to surveil (Lupton & Williamson, 2017). Lupton and Williamson point out that “Dataveillance now frequently operates with the use of digital technology and takes place at varying degrees of people’s knowledge and consent” (p. 782). They should also consider issues related to the effectiveness of identification from facial recognition technology, particularly for students of color (Yoder-Himes et al., 2022).

With regards to dataveillance, educators should work to use technology and data for students’ benefit without opening students to harm. Logistically, this can mean helping students understand what is (and is not) monitored; when surveilled, or even when they simply think they are being surveilled, students may alter their behaviors. This may be good in some situations (e.g., avoiding inappropriate websites), or it could be counter to their academic development (e.g., working in contexts of increased anxiety about performance). Helping students understand what technology can and cannot do is an important component of developing their capacity for critical thinking and for responsible technology use. Finally, leaders need to be transparent with parents and the community about platforms being considered or implemented and be forthright about what data are collected, how they are stored, and for what purposes they are used (Barnes, 2015).

Allegations of cheating are serious, though offenses and responses vary with student age, development and context. A principal dealing with a second-grade student who falsifies a parent's signature on a reading log or a fourth-grader who sneaks a peak at notes for a state capitols test is likely to be engaged in more teaching and redirection as much as assigned disciplinary consequences. As students progress, so do the stakes attached to assessments. State-mandated exams have stringent monitoring practices, so too do exams connected with certifications or particular professional endorsements. Cheating in these contexts is very serious and may affect student opportunities and employability in future endeavors. Further, a false accusation of cheating risks broken relationships among educators, students, and their families, so it’s important to use good judgment in concert with as much evidence as possible, rather

than accept a flagged assessment as proof positive of academic dishonesty.

Leadership Practices & Data Use

Beyond aligning with data safety practices (e.g., using only properly vetted and approved apps and platforms, safe password storage, and two- or multi-factor authentication for accessing any data sets that include PII), leaders should emphasize good pedagogy and underscore the purpose of assessment. That is, teachers cannot know a student's strengths and weaknesses without frequent and accurate assessment; they cannot know how to take a student to the next stage in a learning progression. If a student turns in work that is not theirs, the teacher cannot assess, plan, and respond appropriately. Educators therefore can work to make many assessments "lower stakes" and to engage students as partners in their own learning.

Students cheat for various reasons and sometimes do so unintentionally or rationalize their actions as not really cheating (Waltzer & Dahl, 2023). Recognition of effort and improvement, rather than simply attaining a threshold passing percentage, timely, actionable feedback and avoiding rewards based purely on grades (e.g., allowing only students who pass the unit exam to have extra recess) may press against perceived pressures to engage in academic dishonesty. When possible, project-based or other assignments that require students to use knowledge and skills in ways uniquely relevant to the student can hedge opportunities to cheat. Very little is "cheat proof" but sometimes below-par teaching structures (such as asking the same final exam question every semester or reusing the same quiz year after year) do lend themselves to targeted cheating, whereas other pedagogical structures reduce incentives to engage in academic dishonesty (e.g., Hilliger et al., 2022).

If an app or other platform is used, leaders need to ensure appropriate training for faculty and staff (Attai, 2019). This not only includes appropriate submission/reporting procedures and data safety practices but should also explore approaches to intervention if cheating is suspected or flagged in a system. Beginning an investigation of suspected cheating by questioning–and remaining open to the possibility that the student did not cheat as much as possible–will likely lead to an accurate accounting of what happened, as opposed to a confrontation and accusation of cheating based only on the platform's reporting alone. After all, the platforms may flag indicators the platform considered suspicious or indicative of cheating, but it is still the educator's responsibility to collect a broader set of facts and act on them responsibly.

Finally, and perhaps most importantly, leaders need to "emphasize the humans in the loop," as a recent report from the U.S. Department of Education's Office of Educational Technology (2023, pp. 53-54) suggests. Technology-and perhaps especially AI–should be something explored and implemented with educators–it should not be something with which they are forced to contend without meaningful input. As AI tools evolve, some may prove more constructive than others, but all will require that teachers engage with students around safety, privacy, appropriate and constructive use, and limitations. Humans (district and school leaders, teachers, students, parents/family members) must be ready to "steer" the technology, rather than setting the technology loose and hoping for the best. Leaders play a critical role in how AI and academic integrity tools are introduced, explored, used, and monitored.

References and Resources

- Barnes, K. (2015). The challenge of data privacy. *Educational Leadership 73*(3), 40-44.
- Hilliger, I., Ruipérez-Valiente, J. A., Alexandron, G., & Gašević, D. (2022). Trustworthy remote assessments: A typology of pedagogical and technological strategies. *Journal of Computer Assisted Learning.*https://onlinelibrary.wiley.com/doi/pdf/10.1111/jcal.12755
- Lupton, D. & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *new media & society* 19(5), 780-794. https://doi.org/10.1177/1461444816686328
- Merk, L., (2022). *Federal Court deems university's use of room scans within home unconstitutional.* Future of Privacy Forum. https://fpf.org/blog/federal-court-deems-universitys-use-of-room-scans-within-the-home-unconstitutional/
- Ogletree v. Cleveland State, No. 1:21-cv-00500, 2022 WL 3581569, at *2 (N.D. Ohio Aug. 22, 2022) https://www.govinfo.gov/content/pkg/USCOURTS-ohnd-1_21-cv-00500/pdf/USCOURTS-ohnd-1_21-cv-00500-0.pdf
- U.S. Department of Education, Office of Educational Technology. *Artificial intelligence and future of teaching and learning: Insights and recommendations.* https://www2.ed.gov/documents/ai-report/ai-report.pdf
- Waltzer, T. & Dahl, A. (2023). Why do students cheat? Perceptions, evaluations, and motivations. *Ethics & Behavior 33*(2), 130-150. https://doi.org/10.1080/10508422.2022.2026775
- Yoder-Himes, D. R., Asif, A., Kinney, K., Brandt, T. J., Cecil, R. E., Himes, P. R., Cashon, C., Hopp, R. M. P., & Ross, E. (2022). Racial, skin tone, and sex disparities in automated proctoring software. *Frontiers in Education 7.* https://doi.org/10.3389/feduc.2022.881449

Facilitator's Guide: Balancing Student Privacy and Academic Integrity

Teaching Notes and Considerations for Scenario Facilitators:

In this scenario, leaders must consider the need to protect student data as this responsibility intersects with efforts to promote academic integrity. When data are captured by proctoring or plagiarism software and stored on computers, apps, or other devices, the data must be protected to mitigate the risk of breach or other loss of confidentiality. "Balancing Student Privacy and Academic Integrity" provides scenario users an opportunity to explore various approaches to cheating detection and prevention as these intersect with data security and student privacy concerns.

Extending Activities

- Explore several (3 to 5) academic integrity focused tools/platforms online. You might explore "academic integrity platforms," "anti-cheating software" or "proctoring software" as a start. Compare and contrast facts of the platforms, from cost to what data are collected and how/to whom reports are delivered.
- Roleplay a conversation between Dr. Abby and a parent who is concerned that they have heard that the school will be implementing proctoring software that requires a camera to remain on during an assessment. Among other concerns (generate several prior to the roleplay) the parent is concerned that the required software records keystrokes and will need to be installed on a family computer used by multiple individuals in the home.
- Brainstorm approaches promoting academic integrity that are pedagogical in nature.

Data Dashboards & Early Warning Systems

Learning Objectives

- Understand privacy constraints and ethical guidelines for using technology applications such as status/early warning dashboards fed from district data systems.
- Understand the benefits and limitations of proxy measures as indicators of likely student outcomes.
- Describe the pros and cons of using early warning systems in working with students.

District leaders in the Luna School District have been concerned about students falling behind (e.g., on-time graduation, course failure rates, state exam trends) and have been exploring how data might provide timely insights into student progress and performance. In response, the district made a major investment in a comprehensive data analytics platform which they refer to as their "Data Dashboard" or simply "Dashboard." The Data Dashboard allows the district to integrate data from multiple systems including the student information system (SIS), learning management system (LMS), assessment platforms, IEP and 504 compliance, content filter student alerts (including self-harm and physical threat), and instructional applications that track skill-based mastery. Of particular interest to the district is the Dashboard's algorithm used to identify at-risk students. The algorithm uses attendance, discipline events, nurse visits, content filter data, assignment grades, and skills mastery to build a student at-risk score. After several weeks of data collection, a student profile is developed and a graphical representation of students is displayed based on access level.

Building administration and counselors have a Dashboard that shows at-risk trends by the student. A green arrow is used to indicate students who are improving (decrease in at-risk score) and a red arrow is for students whose score is increasing. The top twenty-five "At-Risk" students, calculated by total at-risk score, are identified. In addition, the top twenty-five "Students to Watch" are calculated by the highest percentage increase in at-risk scores. In addition, the Dashboard can be used to assess sub-group performance on benchmark assessments and classes. The teacher Dashboard shows similar trends.

However, the data they see is based only on the grades and skills they have assessed, attendance for their class, and office referrals they have made. Teachers do not see analysis of data from other classes, nurse visits, IEP/504 goals, or the content filter.

Other access profiles include special education case managers, IEP facilitators, extracurricular sponsors/coaches, students, and parents/guardians, among others. Each profile type is restricted only to analyzing data they have a "need to know." A user may have more than one profile. For example, a teacher may have a teacher-level access profile (for their own students of record), a coach profile (for students who are members of teams they coach), and a parent/guardian profile (for their own children enrolled in the school).

After several months of implementation, Police Chief Marks approaches the high school principal, Mr. Scott, about how they may collaborate to help identify at-risk students in the communication

to offer them early intervention support. Chief Marks is especially interested in the ability to use attendance data, office referrals, and content filter alerts in determining escalating and/or at-risk behavior. These behaviors may include self-harm, community violence, or school violence.

Discussion Questions

- If you were a school principal, and Chief Marks presented his request to you, how would you respond and why?
- What are the benefits and limitations of using predictive analytics? How, if at all, should predictive analytics/early warning systems be used in schools?
- Does the mere analysis of data from varying sources pose an ethical or compliance concern?
    - Are there specific data systems that introduce a higher level of risk/concern?
    - How might the use of the data impact ethical or compliance concerns?
- What risks does a school run having so many kinds of access granted to so many personnel? How can the risk of someone misusing their access to data be mitigated?
- What are some issues with using content filter alerts, office referrals, and nurse visits as indicators of at-risk students?
- Assess whether it would be appropriate for the principal, Mr. Scott, to be able to use the at-a-glance dashboards to spot-check grades, benchmark scores, discipline, and/or attendance for the following groups. For each, justify your response and note what additional consent or documentation (if any) would be needed for access.
    - Basketball team members at the end of a grading period
    - Ninth graders at the end of the fall term
    - Other students in Mr. Scott's daughter's English III class, to see how the teacher scored other students' essays compared to his daughter's.
    - Students involved in the spring play (at the request of the theater teacher)
    - All students, disaggregated by race
    - Students from the travel baseball team Mr. Scott coaches
    - All students, on behalf of the campus SRO, to identify students likely to enter alternative education placements in the absence of SRO intervention
    - All students, disaggregated by free/reduced-price lunch status
    - Students from Mr. Scott's spouse's youth group at church.
    - All students, disaggregated by English language proficiency
    - All students, disaggregated by special education status

From the Evidence Vault:

- Bowers, A. J. (2021). Early warning systems and indicators of dropping out of upper secondary school: The emerging role of digital technologies. In *OECD digital education outlook 2021: Pushing the frontiers with AI, blockchain, and robots* (pp. 173-194). OECD.
- Mandinach, E.B. & Abrams, L. M. (2022). Data literacy and learning analytics. In C. Lang, G. Siemens, A.F. Wise, D. Gasevic, & A Merceron (Eds.). *Handbook of learning analytics*, (pp. 196-204). Society for Learning Analytics Research (SoLAR).
- Reidenberg, J. R. & Schaub, F. (2018). Achieving big data privacy in education. *Theory and Research in Education 16*(3), 263-279. https://journals.sagepub.com/doi/pdf/10.1177/1477878518805308
- Snipes, J., & Tran, L. (2016). *Early indicators and academic mindsets in the Clark County School District*. San Francisco, CA: REL West @ WestEd

In the News / In the World of Practice:

- Backenstoe, K., & Krempasky, K. (n.d.). *The role of learning management systems in middle schools.* https://www.amle.org/the-role-of-learning-management-systems-in-middle-schools/
- Feathers, T. (2023, April 27). Takeaways from our investigation into Wisconsin's racially inequitable dropout algorithm. *The Markup.* https://themarkup.org/the-breakdown/2023/04/27/takeaways-from-our-investigation-into-wisconsins-racially-inequitable-dropout-algorithm
- Herold, B. 9 (2019, May 30). Schools are deploying massive digital surveillance systems: The results are alarming. *Education Week.* https://www.edweek.org/technology/schools-are-deploying-massive-digital-surveillance-systems-the-results-are-alarming/2019/05
- Herold, B. (2021, September 27). Privacy group cautions schools on technology that flags children at risk of self-harm. *Education Week.* https://www.edweek.org/technology/privacy-group-cautions-schools-on-technology-that-flags-children-at-risk-of-self-harm/2021/09
- Nagel, D. (2017, April 25). Study: Tech-enabled early warning systems can have positive impact on chronic absenteeism and course failure rates. *THE Journal: Transforming education through technology.* https://thejournal.com/articles/2017/04/25/study-tech-enabled-early-warning-systems.aspx
- Sparks, S. D. (2022, May 18). With so many kids struggling in school, experts call for revamping "early warning systems." *Education Week.* https://www.edweek.org/leadership/with-so-many-kids-struggling-in-school-experts-call-for-revamping-early-warning-systems/2022/05

Data Privacy and Compliance Considerations

Teachers, parents, students, and administrators clamor for convenience and communication about student progress. A well-designed learning management system

(LMS) can be a part of convenience regarding communications about assignments, grades, and other pertinent metrics (Bouchrika, 2023). Early warning dashboards–drawing on data from student information systems and LMS–can provide convenient and actionable information for educators at multiple levels of a system (Nagel, 2017). At the same time, leaders must be diligent in ensuring systems are compliant with data protection and that contracts and memoranda are clear so that vendors specify what data are collected, how they are stored, who may access and use data, how/for what period collected data are maintained, and for what other purposes (if any) data may be (re)used. Parents and legal guardians must be informed about these data collection/use practices, which in some cases may require explicit consent for the use or the ability to opt out of data collection (for example, with mental health/wellness data).

Beyond appropriately crafted vendor agreements, leaders are also responsible for ensuring processes that limit access to persons with legitimate educational interests, whether those persons are employees, vendors, or community partners. In the scenario above, providing some data to near-peer mentors might be acceptable, with consent from parents of students participating in the program or with privacy agreements and onboarding of the near-peer college students.

Dashboards, LMS, student information systems, and early warning systems can provide convenient, actionable data for educators. At the same time, convenience is no excuse for failing to implement privacy protection processes and safeguards. Responsible leadership for privacy, both in terms of compliance and ethics, require leaders to engage in intentional, transparent communication about all the types of information that are collected, and to seek appropriate consents where needed for the collection, use, and dissemination of such data. This is particularly important when it comes to the kinds of data systems may collect, but which aren't typically at the forefront of students' or parents' minds when they think about data collection in school. For example, students and parents likely think of an LMS as housing grades, assignments, attendance, and feedback; they may not consider logs of students' webpage access, the content of emails sent within district systems, or communications sent outside of school hours through district-owned technology. They likely do not consider data potentially captured by some early warning systems established to flag terms considered signs of risk (see Herold 2019 and 2021), so if school leaders are considering these kinds of systems, they need to tread carefully and with particular attention to vendor agreements as well as potentially undesirable or even harmful consequences of implementation.

School leaders must also be clear about data retention and sharing policies and communicate appropriately with students and families about these policies. In conjunction with district policies, they must ensure that families provide consent where needed (or that systems appropriately constrain data collection/sharing when families do not consent). To be clear, consent is not required for all data collection in schools via LMS or SIS, as most data collected are typical educational data, restricted to internal use or use by external parties on request, and (typically) under the condition of de-identification. However, when data begin to move into the mental health space, or when disciplinary/conduct data may be shared with external parties, and a contract stipulates sharing of those data with law enforcement or other external agencies, parents need to be in the know and have a substantial say in whether and how their child's data will be collected, stored, and shared.

Ethics and Norms

This scenario raises a few ethical considerations pertinent to data use and privacy. First, a major issue in this scenario is the need for transparency about what data are being collected and how they will be used. Teachers collecting time on task data through a technology application is not inherently inappropriate, especially given the relationship between the metric and potential failure or at-risk performance levels. Ethically, educators should be upfront and transparent about what they are collecting and why. The intent is not to surveil students but to identify students needing assistance through data that only the LMS can collect. At the same time, educators should endeavor to use data that are reasonably linked to what is being measured. Time or frequency logged into the LMS may or may not provide an adequate measure of engagement. Students can game this metric easily by logging on but failing to attend to content within the LMS. As with all ethical data use, educators should try to triangulate or at least use multiple measures (including talking with those involved) to gain a clearer picture before making assumptions about the root causes of underperformance.

A second ethical concern surrounds the ability of users to access various profiles when some profiles may privilege them with access to information that they would not typically have while doing legitimate educational business. For example, just because certain employees (like the principal) can access data does not mean that they should–the purpose of access has to meet FERPA requirements. It's acceptable for Mr. Scott to access reports (including early warning system indicators) for students by special education status, race/ethnicity, or grade level, for use in school planning and improvement efforts. It would not be ethical (or within FERPA constraints) to access data on students on his travel baseball team or in his spouse's youth group. These would not be appropriate avenues of access if he were not the principal, so school leaders need to impress on those with system access that it's not sufficient to safeguard passwords and access only data to which they are privy; they should still match access with legitimate educational purpose within the scope of their professional roles. Along the same lines, professionals who have dual or multiple profiles (for example, as a parent, and as an administrator) should only access data pertinent to their goals within their role and specific to the appropriate profile.

Another ethical issue that should be considered, particularly with regard to early warning systems (EWS), is that leaders must push back against tendencies for warning levels (particularly color-coded systems) to become shortcuts to labeling students. Data may suggest an increased likelihood of an outcome that is true for a set of aggregated data, but data does not mean destiny for any one student. Simply because most students with 15 absences in a semester may tend toward a likelihood of dropout does not mean this is true of every student: Some may have very legitimate reasons for the absences, so it is still important to pull the curtain back on data points that feed early warning systems to get to an accurate picture to inform action. Similarly, leaders need to model pushing back on deficit thinking and subtractive language that tends to group students who belong to a group that systems suggest are at greater risk for underperformance, dropout, or disciplinary consequence. If educators start to treat the indicators as destiny (for example, inferring that students in the "yellow" or "red" for disciplinary infractions will likely be troublemakers), they could end up responding to those students in a way that creates a kind of self-fulfilling prophecy. Suppose educators treat students "likely to drop out" or "likely to end up in alternative placements" as if these are inevitable states, rather than indicators to dig deeper

and potentially work through interventions. In that case, they may engage in consciously or unconsciously biased treatment of these students and groups, undercutting the intent of the EWS.

Finally, leaders must be extremely cautious about engaging with mental health data and EWS (see Collins et al., 2021). First, mental health data has the potential, if not treated as sensitive data, to be stigmatizing to those it may be intended to help. Second, EWS does not have a consistent track record for accurately identifying students in crisis (Collins et al., 2021; Herold, 2021). Overreaction can lead to overly invasive school action in the home, harming students (through unnecessary stigmatization) and family rights to privacy. The intent behind collecting and using EWS with regard to student well-being and safety may be good. Still, schools must be cautious and transparent about efforts to collect and use data when the risks of harm from overreach are so great.

Leadership Practices & Data Use

Leaders have responsibilities to protect students without unduly compromising privacy protections, and to ensure that appropriate measures are in place to communicate to staff, students, and families what data are collected, how they are used, and how those data are protected. They also have to ensure that district policies related to consenting procedures related to data collection and use and procedures in place to ensure FERPA compliance is understood and followed. If, in the above scenario, counselors wanted to press forward with adding capabilities to the system to capture indicators of mental health, Mr. Scott would need to not only collaborate with district leaders and IT to ensure appropriate policies and protections are written into vendor contracts or data sharing agreements. Still, he would also need to obtain appropriate consent or permissions if the school wanted to share data with external agencies if indicators trigger safety alerts. The system may be worthwhile, but diligence and preparation need to occur prior to any expansion or rollout to mitigate undue risks of privacy-related harms.

If, in the scenario above, teachers and leaders wanted to collaborate with the university-based near-peer mentoring program, Mr. Scott would need to ensure that appropriate protections and documentation are completed (including, potentially, parental consent) to permit data sharing about the students participating/receiving the mentoring intervention (e.g., Cotto & Siegl, 2021; US Department of Education, 2016). While the school official exception may be appropriate in this instance and permissible with agreements limiting disclosure or use outside of designated purposes, the wise practice would suggest transparency and seeking parental consent whenever possible or, if using the school official exception, notifying parents of the program and communicating what information is collected, used, and shared with program personnel (see Cotto & Siegl, 2021). Consent may be particularly critical if data related to disability is pertinent to providing services, as IDEA has privacy protections that sometimes go beyond FERPA requirements (US Department of Education, 2016).

Leaders also have a responsibility to ensure that appropriate measures are used in assessing engagement and learning. While logging into an LMS regularly may be a good habit to help students develop, using minutes spent on an activity–or minutes logged into an LMS–is at best an imperfect metric for assessing robust engagement. This measure, alongside others (e.g.,

grades, conversations with students, exit tickets) can inform more accurate inferences about student engagement and learning in ways that help teachers engage in appropriate next steps. In the above scenario, if Mr. Skipper focused only on students that log LMS minutes for extra help, he could miss out on students who need intervention and inadvertently provide additional assistance to some who don't need it at all–they just happened to have less time logged in the system. His plan to combine time in the LMS with attendance is more promising, as research has shown that attendance is one of several indicators related to students at risk of failing (e.g., Baker et al., 2020). Leaders should help teachers and staff learn to interpret data points and EWS indicators in concert with other factors to increase the likelihood of appropriate interventions.

Finally, leaders have a responsibility to use EWS and data in culturally responsive ways. Part of culturally responsive school leadership is pushing back on deficit frames, and questioning how structures and language may end up reifying rather than breaking down stereotypes (Khalifa, 2020; Khalifa et al., 2016). For example, if the EWS shows a persistent gap between White and Hispanic students, culturally responsive leaders will seek to determine the root contributors of these patterns and address those. In contrast, those who take surface inferences may buy into stereotypes that Hispanic students are twice challenged by language barriers (when not all are) or that their families prioritize education less. Refusing to buy into simplistic and stereotype-based explanations of gaps is an important facet of appropriately using data-based EWS (Datnow & Park, 2015, 2018).

References and Resources

- Baker, R. S., Berning, A. W., Gowda, S. M, Zhang, S., & Hawn, A. (2020). Predicting K-12 dropout. *Journal of Education for Students Placed at Risk 25*(1), 28-54. https://doi.org/10.1080/10824669.2019.1670065
- Bouchrika, I. (2023, Feb. 23). *Best LMS for schools in 2023: Key features of the top learning management systems*. https://research.com/education/best-lms-for-schools
- Collins, S., Park, J., Reddy, A., Sharifi, Y., & Vance, A. (2021, September). *The privacy and equity implications of using self-harm monitoring technologies: Recommendations for schools.* Future of Privacy Forum. https://studentprivacycompass.org/resource/self-harm-monitoring/#anchor-link-11
- Cotto, J. & Siegl, J. (2021, September). *When schools share data with afterschool programs.* Future of Privacy Forum. https://studentprivacycompass.org/resource/when-schools-share-data-with-afterschool-programs/
- Datnow, A. & Park, V. (2015). Data use for equity. *Educational Leadership 72*(5), 49-54.
- Datnow, A., & Park, V. (2018). Opening or closing doors for students? Equity and data use in schools. *Journal of Educational Change 19*, 131-152. https://doi.org/10.1007/s10833-018-9323-6
- Herold, B. 9 (2019, May 30). Schools are deploying massive digital surveillance systems: The results are alarming. *Education Week.* https://www.edweek.org/technology/schools-are-deploying-massive-digital-surveillance-systems-the-results-are-alarming/2019/05

- Herold, B. (2021, September 27). Privacy group cautions schools on technology that flags children at risk of self-harm. *Education Week*. https://www.edweek.org/technology/privacy-group-cautions-schools-on-technology-that-flags-children-at-risk-of-self-harm/2021/09
- Khalifa, M.A. (2020). *Culturally responsive school leadership*. Harvard Education Press.
- Khalifa, M.A., Gooden, M.A., & Davis, J.E. (2016). Culturally responsive school leadership: A synthesis of the literature. *Review of Educational Research 86*(4), 1272-1311. https://doi.org/10.3102/0034654316630383
- Nagel, D. (2017, April 25). Study: Tech-enabled early warning systems can have positive impact on chronic absenteeism and course failure rates. *THE Journal: Transforming education through technology*.
- Student Privacy Policy Office (2014). *The Family Educational Rights and Privacy Act guidance on sharing information with community-based organizations*. U.S. Department of Education. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/ferpa-and-community-based-orgs_2021.pdf
- U.S. Department of Education (2016). *Data-sharing tool kit for communities: How to leverage community relationships while protecting student privacy*. Washington, D.C. https://www2.ed.gov/programs/promiseneighborhoods/datasharingtool.pdf
- U.S. Department of Education (2023). *Artificial Intelligence and the Future of Teaching and Learning*. Washington, D.C. https://tech.ed.gov/ai-future-of-teaching-and-learning/

Facilitator's Guide: Data Dashboards & Early Warning Systems

Teaching Notes and Considerations for Scenario Facilitators:

In this scenario, leaders are provided an opportunity to consider approaches to systems that provide access to a broad range of individual and aggregated data, including dashboards and early warning systems, and to explore the benefits and challenges of using such systems while also balancing students' and families' rights to privacy. They are challenged to consider the appropriate use of dashboards and early warning systems and situations in which misuse or misinterpretation of such tools may contribute to deficit thinking around students (individuals and groups of students with shared characteristics or system labels). While scenario users may identify additional connections to data use, privacy, ethics, and leadership not addressed in the teaching notes, we point out several areas facilitators can highlight as they lead groups in analyzing the "Data Dashboards & Early Warning Systems" scenario.

Extending Activities

- Assume the district presented its plan to you before adoption. Consult your district's technology and data policies and formulate a response, remembering your dual goals of getting educational data needed to serve students to appropriate personnel and complying with privacy protections. What issues would need to be addressed in your plan/response? How would you address those in line with existing policies? Do you notice any gaps in the policies you review?
- Debate the ethical ramifications of teachers or other educators being able to track student webpage access 24 hours per day (i.e., any time logged in using the district-owned account). Is there a limit to what data systems should collect? When, if ever, do efforts to support and protect students cross a line from monitoring to the invasion of privacy?
- Debate the ethical ramifications of using predictive analytics for reporting and/or intervention related to discipline, attendance, grades, and test scores.
- Some early warning systems go beyond typical metrics like attendance, grades, and course completion and seek to address issues of student safety, well-being, and mental health. Explore some of these tools, and discuss the potential legal and ethical ramifications of collecting, accessing, and using early warning systems linked to such nonacademic indicators. What might you consider in terms of process and privacy protections?
- Read the 2023 U.S. Department of Education Office of Educational Technology's policy report, *Artificial Intelligence and the Future of Teaching and Learning: Insights and Recommendations*, (See Resource section). How might the recommendations in the report be applied to this scenario?

Data Displays & Data-Driven Celebrations

Learning Objectives

- Outline the benefits and potential risks or actual harms of displaying student data, or progress indicators in ways that other students, school employees, and campus visitors can access the displays.
- Outline benefits and potential risks or actual harms of student data displays or similar graphic indicators of progress being publicly recognized through assemblies and rewards.
- Discuss the risks and benefits of holding various celebrations or awards ceremonies based on various types of data (high stakes testing data, personal goal attainment, threshold challenges, attendance competitions, etc.)

Elmwood School District has a new superintendent who encourages the systematic use and reporting of data regularly. Throughout the district, schools have implemented data displays in classrooms and hallways. These "data walls," as many educators refer to them, visually display student progress and outcomes in various ways, which vary by campus. Several are designed to allow tracking/movement of tokens or icons as students or classes progress (e.g., books read, scores on math/reading assessments). In addition, the schools hold achievement celebrations at regular intervals, which sometimes coincide with display data.

The following is a sample of displays observed during recent learning walks, in which leadership teams visit other campuses to learn about and discuss instructional practice, as well as celebrations held by the schools.

1. Classroom A has a bulletin board depicting mountain climbers moving up a mountain from an average score on the beginning-of-year mathematics assessment through several benchmark assessments to an end goal of 85%+. No names appear on climbers, though it is obvious that each student has decorated a climber, many of which seem to sport particular hairstyles and clothing.

2. In Classroom B, there is a "high-frequency words mastery" chart. On the chart, each student has a decorated clip with their first name and last initial. Some clips are near the top of the list--moving close to the goal of 200 high-frequency words. Most are in the middle, and two linger near the bottom, below 20 words mastered.

3. In School C, reading progress boards were displayed in the hallway outside each classroom. These boards sported pictures of various planets, colored by students, with stars added for each book read. A key clarified that a green star equated to a picture book, a red star for a book on the child's "instructional" level, and a gold star for a book at or above the child's "independent" level. Each student had a goal of 100 books read for the school year, with no more than 15 picture books.

4. School D has a stoplight system to visualize progress toward math benchmarks. Just outside the doorway of each classroom is a "red light/yellow light/green light" display with small round stickers (red, yellow, and green) that are placed within the corresponding

"light" on the graphic. The title is "October Mathematics Benchmark." As students, staff, and visitors move about the school, they can quickly assess how many students performed well on the assessment (green), scored near the passing threshold (yellow), or below expectations (red). Outside three rooms, the stickers have numbers written on them.

5. At School E, the kindergarten and first-grade classrooms have a green/yellow/red behavior chart hanging in the classroom. This chart is not easily viewable from the hall or doorway. Each student has a clip, with the student's first name and last initial written on the clip. Students move up and down the chart throughout the day. Each student marks in their binder where their pin is at the end of each day. Students in yellow or red receive a note home to encourage teacher-parent communication.

6. In preparation for state assessment, School C holds a state testing pep rally. During this assembly, they give certificates to students who scored proficient on the previous year's assessment. Special recognition is given to students who scored perfectly in each category.

7. Each semester, School D holds an academic celebration for students who met their goal on the school's benchmark assessment. Students who met their personal goals, set in collaboration with their teacher, participated in a popcorn and movie event. Students who showed growth of 20 or more percent over the previous year's score earned an ice cream and dance party.

Discussion Questions

- What data does your district/school/classroom currently have on display? Is that data similar to any of the examples above? How are students identified on the display, if at all?
- How might data displays be used for motivation and goal tracking without violating a student's right to privacy? What kinds of data would be "safe" to include, and which data should not be shared?
- Other than FERPA protection, what ethical considerations must be evaluated before creating a data display?
- At what point is a data display properly de-identified? Some displays use no identifiers, some use numbers, and some use names. Which, if any, pose threats to student data privacy? Which do not pose direct threats to privacy, but could have other unintended negative consequences?
- Does a display in a hallway or other gathering area have different considerations than one in a classroom?
- For each of the above examples, which displays/celebrations pose a data privacy violation risk? What adjustments might reduce the risk?
- Since all visitors, including parents, must check in at the front office, does this mitigate any privacy violations with how the data were posted in various locations in the school?

From the Evidence Vault:

- Farrell, C.C., Marsh, J.A., & Bertrand, M. (2015). Are we motivating students with data? *Educational Leadership 73*(3), 16-21.
- Harris, L., Wyatt-Smith, C., & Adie, L. (2020). Using data walls to display assessment results: A review of their affective impacts on teachers and students. *Teachers and Teaching 26*(1), 50-66. https://doi.org/10.1080/13540602.2020.1739018
- Marsh, J.A., Farrell, C.C., & Bertrand, M. (2016). Trickle-down accountability: How middle school teachers engage students in data use. *Educational Policy 30*(2), 243-280. https://doi.org/10.1177%2F0895904814531653

In the News / In the World of Practice:

- Hall, L. (2016, May 19). This ed-reform trend is supposed to motivate students. Instead, it shames them. *The Washington Post*. https://www.washingtonpost.com/posteverything/wp/2016/05/19/data-walls/
- Llopis-Jepsen, C. (2015, January 15). USD 501 reaches settlement with top official on leave. *The Topeka Capital-Journal*. *https://www.cjonline.com/story/news/education/2015/01/15/usd-501-reaches-settlement-top-official-leave/16642734007/*
- Nazerian, T. (2018, September 7). Tear down that wall? Why data walls may cause more harm than good. *EdSurge*. https://www.edsurge.com/news/2018-09-07-tear-down-that-wall-why-data-walls-may-cause-more-harm-than-good

Data Privacy and Compliance Considerations

One of the most pressing issues when considering data walls/displays and celebrations are FERPA restrictions on sharing personally identifiable information (PII) with unauthorized persons. Suppose data displays contain students' full names, identification numbers, or enough information that passersby (including leaders in the district or other school district employees who do not hold a legitimate need to know/access the PII) could reasonably identify the student(s). In that case, the teacher and school leader are likely at risk of a FERPA violation (see Future of Privacy Forum, 2021, and Park et al., 2021). This could open the school district to liability should a complaint be filed. There is also a consideration for what information is general knowledge to share in the classroom.

School leaders and teachers should not assume that simply because a display is located inside a school or classroom that it is private. Data displays should never use student names (even the first name and last initial convention can easily be used to identify students).

In the scenario, several displays used numbers (not ID numbers or SSNs); this is a hedge against the risk of student identification. Of course, even if the numbers become easily recognizable (e.g., students share their numbers with each other and through word of mouth the numbers are no longer "coded") or are inadvertently released (e.g., student numbers are also listed on a sticker on students' desks, or correspond to gradebook placement), the information on the displays can become "decodable."

Though using a secured numbering system for data displays may help avoid legal violations of privacy laws, school leaders should consider that doing so may still violate the spirit of privacy policies. An even safer practice would be using stickers or other materials with no identifiers--this can further mask identity.

Ethics and Norms

Beyond legal/compliance considerations, educators should still note the emotional impact on children of walking into a classroom where, for example, a sign at the door announces to all who

pass or enter that multiple students are performing below expectations, while those in the classroom next door are all passing. Leaders should also reflect on the intentional and unintentional signals these kinds of postings communicate to visitors and others in the school about the kinds of students and teachers who inhabit these classrooms.

Without caution, these practices risk running afoul of ethical guidelines. For example, PSEL standard 2(c) notes the leader's responsibility to "Place children at the center of education and accept responsibility for each student's academic success and well-being." In some of the displays presented in this case, it could be interpreted that the data displays were not implemented to support student learning, but to provide a monitoring check on teachers by school leaders and, eventually, the superintendent. Short of a monitoring/accountability goal or a theory of action that holds that students will try harder (i.e., be more motivated) if they do not feel good about their placement on a display, there is little rationale for posting student data so that it can be viewed by persons other than the student, the student's guardians/family, and the teacher. Where data can be helpful is when it is an artifact around which a teacher and student collaborate, in the presence of actionable, meaningful feedback; that can be attained via data folders or chats, apart from classroom or hallway displays that risk student privacy.

Leaders should reflect on what they hope to achieve through the use of data walls; if the actual drivers are more aimed at surveillance (even being able to gain "at a glance" information during districtwide learning walks or classroom walk-throughs/observations) than supporting more in-depth analysis of what is happening in a classroom, they may need to retool or rethink implementation.

Leadership Practices & Data Use

School leaders are, first and foremost, instructional leaders. A primary role of the leader is to ensure that students are afforded high-quality educational experiences; this necessarily involves supporting the broader healthy development of each child in the school. To this end, one consideration for this scenario is whether the data displays are necessary for the goals stated. If there is not a firm instructional reason for these displays to exist, there is likely not a good rationale for creating them. The goal of data is to inform teaching and learning, not to label students. At the same time, teachers may create displays either to motivate students or to use as focal objects for discussion around learning standards and progress (such as anchor charts and self-assessment). Fun displays where classes compete as whole groups against other classes in ways that allow for differentiation and disallow scapegoating (e.g., total minutes read, where students don't know each others' totals) may not present the same privacy concerns, though educators should guard against situations where students can blame others for "losing" such a contest.

Individual data folders (accessible only by teachers, students, parents, and those with an educational need to know) are likely a better option if guided reflection is a goal. Though these are not in use in this scenario, using work samples and guided self-assessment and reflection in alignment with specific learning targets/standards could support student development (Wiliam, 2018) while avoiding some of the privacy risks posed by data walls.

Data use should inform school improvement and spur crucial self-reflection amongst educators at a school (Khalifa, 2020). This is very different from collecting and broadcasting data about students. The latter can reify deficit thinking if leaders are not careful about how they examine, communicate about, and publicize data (see Hammond, 2015). This is not to say that leaders should avoid data when those data reveal gaps in how students are being supported and served; in fact, effective systemic use of data calls for radical self-examination along a number of data points and indicators that help identify strengths and areas in need of improvement for the system (Marzano et al., 2018). However, data must be about how the system is serving students, not the other way around.

Finally, as evidenced by the PSEL and ISTE standards listed at the beginning of this scenario, a responsibility of school leaders is to cultivate and sustain healthy, productive, collaborative relationships with and among all stakeholders–parents/families, students, teachers, and staff alike. To work together these groups must develop a level of trust, and the leader's actions go a long way to building or diminishing trust (Tschannen-Moran, 2014). If data displays are used in ways that (even unintentionally) shame students, teacher and school relationships with students and families will be damaged, and these relationships and connections are critical for supporting student learning and development.

Family members who visit schools only to see their children's names, numbers, or symbols at the bottom of lists or displays in hallways or classrooms could be embarrassed or upset with the school for highlighting their children's deficits in ways observable to others; they could even perceive these as evidence of ineffective instruction. Students who see their names (or symbols, or code numbers) at the bottom of a performance list could become convinced they cannot learn and could give up. They could also be targeted for teasing by other classmates. Teachers required to post benchmark scores using the "stoplight signs" outside their rooms may opt to shut their practice to colleagues–rather than to collaborate–or may even feel pressured to raise scores in unethical ways.

The art of leadership requires leaders to engage in candid data conversations, but in ways that reduce perceived threats to teachers, students, and parents so that problems centered in teaching and learning can be surfaced and addressed. Leaders who use or observe the use of data displays must be thoughtful about how they use these tools, or they could become detrimental to the work of school improvement.

References and Resources

- Hammond, Z. (2015). *Culturally responsive teaching and the brain: Promoting authentic engagement and rigor among culturally and linguistically diverse students.* Corwin.
- Heritage, M. (2007). Formative assessment: What do teachers need to know and do? *Phi Delta Kappan 89*(20), 140-145.
- Khalifa, M. (2020). *Culturally responsive school leadership.* Harvard Education Press.
- Marzano, R. J., Warrick, P.B., Rains, C.L., & DuFour, R. (2018). *Leading a high-reliability school.* Solution Tree.

- Park, J., Cotto, J., Waller Curtis, A., Klein, C. Reddy, A., Siegl, J, Sollberger, A., Triplett, J. & Vance, A. (2021, January 12). *Student privacy communications toolkit: For schools & districts.* Future of Privacy Forum. https://studentprivacycompass.org/resource/student-privacy-communications-toolkit-for-schools-districts/
- Future of Privacy Forum (2021, October 5) *Student privacy primer.* https://studentprivacycompass.org/resource/student-privacy-primer/
- Tschannen-Moran, M. (2014). *Trust matters: Leadership for successful schools* (The Leadership & Learning Center). Jossey-Bass.
- Wiliam, D. (2018). *Embedded formative assessment* (2nd edition). Solution Tree.

Facilitator's Guide: Data Displays & Data-Driven Celebrations

Teaching Notes and Considerations for Scenario Facilitators:

Scenario users will encounter and explore multiple applications of data privacy and ethics. Participants are encouraged to work through discussion questions and engage in the suggested activities, in small groups. While not all applications of data use, ethics, and privacy will be covered by these teaching notes, below we point out several areas that facilitators may choose to emphasize as they lead groups in learning with the Data Displays & Data-Driven Celebrations scenario.

Extending Activities

- Browse Pinterest or another internet-based repository of images and examine pictures of "data walls" or "data folders" shared by users. Assess: What do you see that would benefit students, and how would you say the tool contributes to improved outcomes (i.e., make explicit your theory of action)? What do you see that runs afoul of legal or ethical guidelines for posting student-related data or information?
- Explore district policies on data displays (in classrooms or hallways). If no policy exists, draft guidance that you would share with teachers at your campus/district that aligns with tenets of formative assessment (e.g., Heritage, 2007; Wiliam, 2018) and also complies with FERPA.
- Review a complaint from a parent, who asserted a privacy violation when a school rewarded students who exhibited "growth" on a reading exam. At the same time, students whose scores did not exhibit "growth" were excluded. (See https://www.nysed.gov/sites/default/files/decision-williamson-csd-7.13.22-1.pdf) A similar issue could be raised when some students are rewarded with a field trip or visible recognition for perfect attendance. What about having students who failed an exam stay in at recess and engage in correction or tutoring? In such cases, what constitutes an "award" and thus may fall under directory information, and at what point would the exclusion of a group also reveal protected data about students in that group? Discuss the legal issues at play, and the ethical issues, of public rewards or recognitions based on various data points. How would you guide faculty and staff in using data to determine reward, award, and activity status?

Student Surveys

Learning Objectives

- Outline the benefits and potential risks or actual harms of collecting various data from students through surveys.
- Identify the eight protected categories that trigger certain notification and consent requirements before student participation in surveys under the Protection of Pupil Rights Amendment (PPRA).
- Delineate the notification and opt-out requirements for student surveys, depending on whether participation is required or whether the data collection is anonymous.
- Understand when opt-in is required for surveys.

The Grady School District uses student surveys to improve education, gather opinions, and stay informed on student well-being issues. Over the past week, students at Grady High School have participated in three surveys.

Speech and Debate Class

Students in the speech and debate classes used a handheld student response "clicker" system to report opinions on controversial topics. The clickers were randomly handed to students and no identifying information was submitted; therefore, the responses were considered anonymous. Students were told that they could refrain from answering any questions. After each question, the teacher displayed a responses chart and used the results to guide a classroom discussion.

The activity asked students the degree to which they agree or disagree with statements such as:

- Abortion should be a legally protected right.
- Religious displays on public grounds should be protected under the First Amendment.
- Businesses should be able to refuse service on grounds of religious objection to same-sex relationships.
- Marijuana should be legalized.
- Healthcare is a right that should be provided and protected by the government.
- Gun control laws are violations of the Second Amendment.

School Climate and Safety Survey

All students were sent a link to the school's climate and safety survey through the learning management system. The goal of the survey was to ascertain the students' sense of belonging and perceptions about physical, emotional, and psychological safety on campus and at school-

sponsored activities. Students were provided time during class to take the survey and were allowed not to participate or to participate but skip any question(s) they did not wish to answer. Student names or IDs were not automatically collected; however, students could provide their names if desired.

The initial questions asked students to select their gender, race, ethnicity, gender identity, and sexual orientation. Additional survey questions asked if the student:

- felt they fit in at school
- has been a victim of bullying or harassment based on race or sexual orientation at school
- has been a victim or witness of bullying or cyberbullying in the current school year
- has been a perpetrator of bullying or cyberbullying in the current school year
- has experienced a desire (or made an attempt at) self-harm in the last 30 days

Student Journalism Youth Activism Series

Students in the school's journalism class are working on a series on youth activism.. As part of the story, they distributed a questionnaire asking students about their basic political beliefs, how they would have voted in the last election, what political issues are most important to them, and if and how they have tried to engage in political processes. Because the newspaper intends to use quotes, they collect student names along with each questionnaire but also ask students how they wish any quotes to be attributed with options to stay anonymous. Forty students respond to the survey, most opting only to have their first name or no name associated with any quotes.

Parental Concerns

Mr. Wiggins, principal of Grady High, received a few complaints and concerns regarding the surveys.

- Speech and Debate class: students were polled on political beliefs and engaged in discussions around their beliefs.
- School climate and safety survey: parents were concerned that their students were surveyed about sensitive topics, including sexual orientation, gender identity, and "mental health" (which the parent explained was in relation to a question about self-harm).
- Overall concerns: some parents felt that the types of information included in the surveys/polls amounted to an intrusion into their children's (and by extension, their family's) personal beliefs and behaviors. One parent asks about the purpose of asking such questions to students, how the information will be used, who can access their student's responses, and why these kinds of questions are being asked by or under the supervision of school personnel.

Discussion Questions

- Review the details of the three surveys/questionnaires. Where, if at all, does each conflict with the Protection of Pupil Rights Amendment (PPRA)? Which protected categories might apply to the surveys?
- What makes a survey/questionnaire "anonymous"? How might anonymity be breached due to the technology or the types of questions/items included?
- Does making the survey optional change any of the school's requirements for notification and choice (opt-in vs. opt-out)?
- What makes a survey "optional"? How might peer pressures, perceived expectations from those in authority, or how a survey is actually deployed affect students' ability to respond or to choose not to respond to any survey/survey item?
- Does the Speech and Debate class activity qualify as a "survey" for PPRA purposes? Why or why not? Does it create an undue risk for students who participate (e.g., data privacy)? If so, how might this be mitigated, or the activity adjusted, to protect students?
- Given the details presented, what adjustments (in content, consent process, or delivery/deployment) would you suggest to ensure data collection aligns with PPRA?
- How does the age of student participants/ respondents' figure into an assessment of what processes or constraints apply with regard to surveys and the PPRA?
- In the instances described, the surveys are used for school/instructional purposes. What would the implications be if a survey was not specific to the work required of Grady School District employees? For example, what if any of these surveys were deployed in conjunction with a doctoral student's research project? Or, if the questions in the safety survey were asked by the state health department? How might the leadership team assess the risks and appropriate processes?
- As a building leader, how might the principal ensure all student surveys meet the privacy requirements under PPRA?
- What if the survey did not store IP addresses or other information linking responses to students' devices?

From the Evidence Vault:

- Archambault, S. G. (2021). Student privacy in the digital age. *BYU Education & Law Journal 2021*(1), Article 6. https://scholarsarchive.byu.edu/byu_elj/vol2021/iss1/6?utm_source=scholarsarchive.byu.edu%2Fbyu_elj%2Fvol2021%2Fiss1%2F6&utm_medium=PDF&utm_campaign=PDFCoverPages
- Student Privacy Policy Office (2020, November). *Protection of Pupil Rights Amendments (PPRA).* SPPO-21-01. United States Department of Education. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/20-0379.PPRA_508_0.pdf

In the News / In the World of Practice:

- Hall, S. (2021, December 6). Surveys at NS middle and high schools draw questions, complaints from parents. *NRI Now.* https://nrinow.news/2021/12/06/surveys-at-ns-middle-school-and-high-school-draw-questions-complaints-from-parents/
- Gewertz, C. (2018 May 24). U. S. Ed. Dept. warns districts to step up student privacy protections for SAT, ACT. *Education Week.* https://www.edweek.org/teaching-learning/u-s-ed-dept-warns-districts-to-step-up-student-privacy-protections-for-sat-act/2018/05
- Grizzard,K. (2021, May 27). Parents raise concerns about school district surveys. *The Daily Reflector.* https://www.reflector.com/news/local/parents-raise-concerns-about-school-district-surveys/article_f2a06cb0-9d92-5877-a5e8-1122f1425726.html
- Price, M. L., & Viviani, N. (2017, September 17). Utah teacher on leave for student quiz on sex lives, drugs. *WIBW Channel 13.* https://www.wibw.com/content/news/Utah-teacher-on-leave-for-student-quiz-on-sex-lives-drugs-443947113.html
- Weinberg, T. (2022, June 8). Missouri attorney general subpoenas school districts over student surveys. *Missouri Independent.* https://missouriindependent.com/2022/06/08/missouri-attorney-general-subpoenas-school-districts-over-student-surveys/

Data Privacy and Compliance Considerations

Many educators are well acquainted with the Family Educational Rights and Privacy Act (FERPA) and are familiar with constraints on the types of data in student education records that may be released, under certain conditions, to parents, school personnel, or other officials under limited conditions (Cole, 2021; Future of Privacy Forum, 2021). However, school leaders and other educators might erroneously conclude that if a student's PII is not attached to a survey instrument, there are few to no concerns with deploying student surveys to assess and improve school safety or climate or to deepen understanding of student experiences and needs. They may also think that the school has no input or responsibility for how school personnel introduce surveys deployed by other entities (for example, surveys embedded in standardized tests like the SAT or ACT that collect additional–though optional–data for, among other things, college recruitment efforts or even by educational researchers). These conclusions would be erroneous because whether or not the data collection via survey is anonymous, the PPRA lays out particular responsibilities for school personnel when student surveys inquire about particular kinds of personal information. Specifically, the PPRA lays out eight "protected categories" of information. These eight categories include

1. Political affiliations or beliefs of the student or student's parent;
2. Mental or psychological problems of the student or student's family;
3. Sex behavior or attitudes;
4. Illegal, anti-social, self-incriminating, or demeaning behavior;

5. Critical appraisals of others with whom respondents have close family relationships;
6. Legally recognized privileged or analogous relationships, such as with lawyers, doctors, or ministers;
7. Religious practices, affiliations, or beliefs of the student or student's parent; or
8. Income, other than as required by law to determine program eligibility. (Student Privacy Policy Office, 2020, p. 1).

If items/questions in a survey associated with a school activity or requirement address any of the eight protected categories, the PPRA triggers certain notification and/or consent requirements, which turn not only on the content of survey items but on whether student participation is required. It is important to note that the *school* does not get to decide whether a situation requires parents to "opt-in" or "opt-out" of their child's participation in a survey: consent requirements and the opt-in/opt-out status of an instrument are governed by characteristics of the survey and whether the survey is required, optional, or was created by school/district personnel or a third party. Table 1 provides brief guidance on what action(s) are required. Note: "Covers eight protected categories" should be read "covers *any of the* eight protected categories"; a questionnaire, survey, or data collection instrument need not cover ALL of the protected categories to trigger a school-required action.

Table 1. Decision-making matrix: Student Surveys & PPRA (from Sallay & Vance, 2020)

Student Participation Required	***Covers any of the eight protected categories***	***Opt in/Opt out***
Yes	**Yes**	Provide notice and parents must opt in for the student to take the survey
Yes	**No**	Provide notice and parents have the right to opt-out
No	**Yes**	Provide notice and students have the right to opt-out (but check your specific state law first)
No	**No**	Provide notice only if the survey was created by a third party. In that case, parents have the right to opt-out.

Finally, there are a few additional caveats. The requirement for notice and consent (that is, students' parents must opt them into the survey for a student to participate) attaches to a survey that concerns one or more of the eight protected categories "if the survey is funded as part of a program administered by the U. S. Department of Education" (Student Privacy Policy Office, 2020, pl. 1). However, parents must still receive notice and an opportunity to opt-out if the survey covers any of the protected categories and is:

> *administered or distributed to a student by a local educational agency that is a recipient of funds under an applicable program (LEA) if the protected information survey is either not funded as part of a program administered by the Department [of Education] or is funded a part of a program administered by the Department but to which a student is not required to submit. (Student Privacy Policy Office, 2020, p. 1)*

The PPRA provides that parents are entitled, upon request, to inspect "Protected information surveys and surveys created by a third party, before the administration or distribution by an LEA of the surveys to a student" (Student Privacy Policy Office, 2020, p. 2).

Taken together, the PPRA impacts at least one of the issues at Grady High School (though state law and district policy could affect all three, potentially). First, the school climate/safety survey certainly appears to address some of the eight protected categories. Items inquired about gender identity and sexual orientation, potentially self-incriminating behavior (that is, they were asked if they have been a perpetrator of bullying), and aspects of mental or psychological health (i.e., acts of self-harm). The survey may have been "optional," but as it was deployed during homeroom/advisory time, students may not feel comfortable choosing not to participate when sitting among peers who are participating. Moreover, the survey was deployed through the LMS, so even if IP addresses are not collected, the data will be stored in the LMS and may be accessed by whoever has access/permissions in the LMS.

Finally, open-ended items can threaten the anonymity of responses within the data set collected (housed in and accessed through) the LMS. If a student expands on a response in a manner that identifies the student, then the responses to that survey can no longer be said to be "anonymous" and anyone accessing the data might know, for example, the gender identity, sexual orientation, or victim or perpetrator status of a particular student. The survey may have been developed with the intent to create a safe and positive schooling experience for all students; however, given the nature of the items, the school needed to–at a *minimum*–provide notice to parents (with the opportunity for parents to review the survey) and give the opportunity for parents–not just students–to opt out of the survey. If the issues with the perceived requirement to participate cannot be mitigated, then the school should provide notice and require consent (that is, have parents opt-in) before deploying the survey.

The other two issues presented are not as clear-cut. The clicker system and "controversial subjects" poll in class were not required, and a case could be made that it was a pedagogical tool and not a "survey" in that data were not actually collected nor stored for analysis. Still, given the content of the statements, a wise practice would be for the teacher to communicate with parents, convey the rationale for the exercise and the fact that participation is optional (and anonymous), and provide an opportunity for parents to opt-out. Of course, this creates challenges, too–the only way to ensure a student whose parent chooses to opt-out would be to issue a nonworking clicker or not to issue a clicker at all–something that could embarrass or alienate the student. Still, given the content of the poll and despite the seemingly good fit with the standards of learning established for a speech and debate class, good communication can only build trust with families and underscore how the activity fits with class learning objectives.

The third issue–the journalism class/school newspaper project–is also a gray area. The project clearly concerns a protected category (political beliefs), and depending on students' responses, could conceivably wander into other categories. But is a student interview for a school newspaper story a "protected category survey"? It certainly isn't a systematic survey. Also, the student journalists have established some basic protections to ensure that students can opt to use full or partially identifying information, or no identifying information at all. Participation is also clearly not required, and even though students are conducting "on the spot" interviews, the odds of coercion are lower than students sitting in a classroom, being asked questions as a group, by persons with perceived authority (e.g., teachers and administrators). Here again, this may not fall under PPRA requirements, but (as will be discussed more in the section on ethics), wise practice for the journalism *teacher* would be to communicate about the project with the broader community and let parents have an opportunity to opt-out (with only students whose parents do not choose to opt-out being approached for potential interviews). Of course, the data collected on forms will still be stored somewhere (in students' binders? In a teacher's office) and accessed by journalism students. This creates additional risk because a student who provided frank but potentially unpopular responses (unpopular with peers *or* with parents who read the resulting story) could be harassed or otherwise suffer if their identity and opinions were made known. This is a risk even for students who check "Don't use my name" because the person conducting the interview knows who said what, and thus the interview itself is not anonymous.

The bottom line for PPRA is that parents have a say in protecting their children from being required to disclose certain personal information, and students' personal data–however it is collected and stored–must be protected (Park et al., 2021). School leaders, therefore, need to be familiar with the PPRA and required notification and consent triggers and should also ensure that teachers who may be surveying students in any way related to the eight protected categories are likewise aware of the requirements, including any district policies for survey review and approval.

Ethics and Norms

Schools and school personnel have an ethical responsibility to safeguard students and their data. Sometimes, this may result in what might present as dilemmas. For example, suppose schools cannot ask students about issues related to social-emotional well-being, self-harm, or substance use/abuse. How can they adequately provide programs and resources to support student well-being? But if schools do use surveys that ask for these types of information, they may inadvertently increase the risk to students, particularly if they fail to engage in transparent communication/notification procedures or safeguard student responses.

Student surveys are one pathway to understanding the strengths and needs of a campus or district and can inform programming, improvement plans, and staffing (Marzano et al., 2018). Schools can meet their ethical duties to build safe and welcoming campuses and to mitigate the potential of harm to students by aligning continuous improvement efforts with PPRA and asking some reflective questions to ensure the ethical use of surveys and survey data.

First, educators must work with parents and guardians in authentic partnership (Kyzar & Jimerson, 2018). This means not only complying with rules and policies, but maintaining open lines of communication about what data are collected, why they are collected, and how they are used.

Educators should remember that when they use whole-school surveys, they are examining data for trends. With appropriate deployment and return rates, trends that inform resource allocation and service structures will still result in providing the kinds of services needed to support a healthy school environment, even if some students choose not to participate or are not permitted to participate via parent opt-out.

Second, as to whether the instrument is truly a "survey" as indicated by PPRA or a pedagogical tool (as in the speech/debate class example), one approach is to ask whether these particular questions need to be asked to get the information needed. Returning to the speech/debate example, if the learning objective is to explore how to talk about controversial issues, the teachers could generate items that avoid PPRA categories entirely.

Third, educators should consider hidden pressures that can be coercive to students; students who otherwise wish to avoid survey participation or self-disclosure may act against their own wishes due to peer pressure (as in a case where everyone in homeroom is responding to a survey) or to perceived authority (students may feel like they must comply with a request by a teacher, counselor, or administrator to take an "optional" survey). Providing optional activities (so that students don't know who is taking a survey, who has opted out, or who has been opted out by parents) and deploying surveys at times when students will not notice who is and who is not participating (e.g., lunchtime or over a 72-hour period) are potential approaches for mitigating these pressures.

In the case of the classroom examples, the teachers have an ethical duty to protect student responses, which is most salient in the journalism example. Student journalists will be able to access the forms. A student could access and reveal the identity of a student who provides a quote that reveals sensitive personal information or an unpopular opinion; this could result in bullying or harassment. It is incumbent on the teacher to not only discuss journalistic ethics with students but to develop and implement procedures for collecting quotes and information for stories that cannot be readily re-identified. For example, students could use a code number for participants and quotes with the teacher keeping the only master list, or the teacher could use a two-step process where students who permit their name to be used must also have a parent sign off on using the name in the story. Ethically, educators must also consider that a minor student may see nothing wrong with attaching a name to an opinion or statement that the adult can foresee will cause the student significant problems. Again, maintaining open lines of communication among students, teachers, counselors, administrators, and families, with the best interests of the student in mind, can help navigate challenging situations while honoring student agency and voice.

Finally, ethics require that educators remember that honoring student agency means that even if a parent is notified of a PPRA-implicated survey, if the parent opts in, a student can still decline to participate.

Leadership Practices & Data Use

There are several major questions raised in the scenario that provide school leaders with opportunities for reflection. First, data collection related to school improvement efforts should be framed to inform specific areas of inquiry, research questions, hypotheses, or agreed-upon problems of practice (Hinnant-Crawford, 2020; Mintrop, 2016). Questions should not be posed for mere curiosity. Leaders must also remember that questions requiring self-disclosure (even anonymously) can spark anxiety and push respondents to complete items in ways perceived as socially desirable (Groves et al., 2009).

Data use should inform school improvement and spur crucial self-reflection amongst educators at a school (Khalifa, 2020). This is very different from collecting and broadcasting data about students. The latter can promote deficit thinking if leaders are not careful about how they examine, communicate about, and publicize data (see Hammond, 2015). This is not to say that leaders should avoid data when data reveal gaps in how students are being supported and served; in fact, effective systemic use of data calls for radical self-examination along a number of data points and indicators that help identify strengths and areas in need of improvement for the system (Marzano et al., 2018). However, data must be about how the system is serving students, not the other way around.

Some leaders may wish to collect climate data or social-emotional data and depending on what items are included in a survey, these efforts may fall under PPRA's notification and opt-in/opt-out requirements. This can be done if leaders are intentional about the process from conception through deployment/collection of data and if they attend to the requirements set out in the PPRA. Before launching any school-wide survey, school leaders should engage in appropriate development and/or review. For locally developed surveys, an advisory board of leaders, counselors, teachers, and parents can help identify high-quality or problematic items or areas of inquiry and prevent unanticipated reactions to items considered innocuous to survey developers. If leaders are using a survey that was not developed locally, a review process for content is still appropriate. Still, leaders should also work to ensure that the school holds appropriate permissions for use, as some surveys will be copyrighted and only available with particular permissions or for a fee. Commercially available surveys may be desirable as they are already validated, or a company may provide useful visualizations/data analysis reports.

Whether purchased or locally developed, leaders should not deploy surveys through a platform or private company without abiding by district policies and engaging district leaders to ensure that appropriate contracts and data security agreements are in place to govern the storage, access, and use of collected data. Ignoring this responsibility risks student privacy on multiple levels (Archambault, 2021 and Barnes, 2015).

Finally, school and district leaders should also remember that PPRA guides how particular kinds of information can be solicited from students: Leaders face fewer regulatory constraints when

surveying parents/families for their perspectives around safety, school climate, and student wellbeing, and these surveys can inform instructional, social-emotional, and equity work at schools in myriad ways (see Radd et al., 2021). A good general guide is: Engage in inquiry, and ask what needs to be asked, and of whom it needs to be asked, to support the learning, growth, and well-being of students. At the same time, abide by PPRA and state/district regulations to ensure transparency in communication and in any permissions/consent process as needed.

References and Resources

- Future of Privacy Forum (2021, October 5) *Student privacy primer.* (2021, October 5). https://studentprivacycompass.org/resource/student-privacy-primer/
- Groves, R.M., Fowler, Jr., F. J., Couper, M.P., Lepkowski, J.M., Singer, E., & Tourangeau, R. (2009). *Survey methodology* (2nd edition). Wiley.
- Kyzar, K. & Jimerson, J. B. (2018). Bridging the home-school divide in the middle grades: A process for strengthening school-family partnerships. *Middle School Journal 49*(1), 13-23. https://doi.org/10.1080/00940771.2018.1399331
- Sallay, D. & Vance, A., (2020, March). FAQs: The Protection of Pupil Rights Amendment. *Student Privacy Compass. https://studentprivacycompass.org/faqs-ppra/*
- Student Privacy Policy Office (2020, November). Protection of Pupil Rights Amendments (PPRA). SPPO-21-01. United States Department of Education. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/20-0379.PPRA_508_0.pdf
- von Zastrow, C. (2022, December 8). Measuring students' mental health while protecting their privacy. *EdNote*. Education Commission of the States. https://ednote.ecs.org/measuring-students-mental-health-while-protecting-their-privacy/

Facilitator's Guide: Student Surveys

Teaching Notes and Considerations for Scenario Facilitators:

Given the myriad challenges school leaders face and the impetus to engage in continuous improvement efforts that are inclusive of student voice, student surveys may be at the forefront of school leaders' efforts to understand better the culture, climate, and needs of any school context. Yet even well-intended efforts can run afoul of privacy laws and ethical constraints if school leaders (and leadership teams and teachers) are not intentional about the data they collect and how data collection aligns with (or runs afoul of) laws like the Protection of Pupil Rights Amendment (PPRA). Of course, many districts will have policies that govern the collection of types of data–within or external to surveys–but knowledge of the PPRA provides a foundation to begin a thoughtful, privacy-oriented decision-making process around the construction, deployment, and use of student survey data.

In this scenario, users encounter several iterations of data collection that may or may not align with PPRA, as well as instances that may be legal, but which may still warrant consideration of the ethics around student surveys in schools. While not all applications of data use, ethics, and privacy will be covered by these teaching notes, in what follows we point out several areas that facilitators may choose to emphasize as they lead groups in learning with the "Student Surveys" scenario.

Extending Activities

- Review the policies in place for collecting survey data within your district, in conjunction with the PPRA. Assess how each of the surveys/questionnaires described in this scenario would align with or violate district policy.
- Take the perspective of the principal, Mr. Wiggins, and imagine he has the opportunity to go back in time and review each of the instruments/processes used to collect data before they are deployed. How should he coach the teachers, journalism students, and leadership team to get useful data in PPRA-compliant ways? What questions should he ask, and what suggestions/directives can he provide?
- Craft a response plan for Mr. Wiggins to use as he works to respond to the Wayne family. What questions does he need to ask of whom? Script notes you would use as you compose your response (email or conversation). Either write out the email/response or roleplay the conversation Mr. Wiggins would have with Rosie's parent(s).

Using Free /Reduced Lunch Qualification Status to Assign Student Support

Learning Objectives

- Identify when and under what conditions school personnel may access a student's free/reduced lunch (FRL) qualification.
- Evaluate the kinds of data and data sources that may be appropriate for determining educational interventions and discuss when and why some forms of readily available or easily accessible data may not be a good fit for the intended task.
- Outline benefits and potential risks or actual harms of private, identifiable student-related data being shared, even for well-intended purposes.

The Garden School District technology department's data manager, Kim Powell, has recently received several data requests that have included a student's free/reduced lunch status. The number of requests, including student lunch status, has significantly increased this past year. She will need to defend her decisions regarding including or removing lunch status from the reports provided. To ensure she is not improperly withholding or disclosing a student's status, she creates a list of the requests for review with her district legal counsel.

- Mr. Enzo, principal of Ivy Middle School, requested a list of all students who qualify for free/reduced lunch, along with their last three reading and math scores in the district benchmarking assessment system. He plans to use this information to prioritize tutoring services funded through an agreement with the local university.
- Dr. Greife, assistant superintendent of elementary education, has just received the state assessment results and noticed that the free/reduced lunch subgroup performance was lower than expected. He would like to track the performance of these students to see if curriculum adjustments are improving their benchmark scores. He has requested math and ELA benchmarks from the past two years and a scheduled pull of the upcoming year's benchmark assessments. He will need this data by student but would also like the teacher's name included with each test result.
- The district has just applied for a grant to provide free mobile hotspots for any student who qualifies for free/reduced lunch. The district curriculum team has asked that a report be sent to each principal of students who qualify for this program so they can contact parents to determine interests/needs.
- The district offers discounts on athletic events, technology device insurance, and class fees for students who qualify for free/reduced lunch. The Tulip High School fee secretary asked the information services team to apply this discount for all students who qualify before posting fees.
- The district is looking to build a new elementary and middle school. They have hired a demographer to propose new school boundaries. The demographer has requested a full data set from the school, including student ID, name, race, ethnicity, address, current school, grade, first enrollment date, and lunch status. This data will be used to help reduce the disparity of any subgroup.

- The free/reduced lunch grace period is close to ending for the year, and the food service director has noticed that program participation is lower than in years past. He has decided to draw prizes (TVs, gift cards, and bikes) for all qualified applications approved by the end of the month. He has asked that the data team provide a list of all students who qualified the previous year but have yet to apply this year. In addition to sending a mass email to all district parents, he plans to send backpack fliers home with students who will be removed from the program at the end of the grace period.

Discussion Questions

- Evaluate the ethics, propriety, and rationale for each request that contains students who qualified for free/ reduced lunch (FRL). If you were the data manager, would you fulfill each request as presented?
    - What additional questions might you have?
- What are the risks and benefits of focusing instructional support, tutoring, or other support services on only students who qualify for free or reduced meals?
- Each request includes student-level identification of lunch status. Can the school/district meet the same goal without identifying individual students? What other means might you suggest to the requestor?
- Is FRL a legitimate proxy for socioeconomic status? Why or why not?
- Under what circumstances can individual student lunch status be shared with school personnel? What are the limitations under those circumstances?
- Why is it important to attend to the actual or potential needs of students whose families are near/below the poverty level? What kinds of interventions are supportive, and what strategies might schools use to identify and meet needs without stereotyping, shaming, or making unfounded assumptions about student or family needs?

From the Evidence Vault:

- Atwood, E. D., Jimerson, J.B., & Holt, B. (2019). Equity-oriented data use: Identifying and addressing food insecurity at Copper Springs Middle School. *Journal of Cases in Educational Leadership 22*(3), 70-84.
- Darling-Hammond, L., & Cook-Harvey, C.M. (2018). *Educating the whole child: Improving school climate to support student success.* Learning Policy Institute. https://files.eric.ed.gov/fulltext/ED606462.pdf
- Fergus, E. (2019). Confronting our beliefs about poverty and discipline. *Phi Delta Kappan 100*(5), 31-34.
- Fortner, K. M. Lalas, J., & Strikwerda, H. (2021). Embracing asset-based school leadership dispositions in advancing true equity and academic achievement for students living in poverty. *Journal of Leadership, Equity, and Research 7*(1), 1-19. https://files.eric.ed.gov/fulltext/EJ1288402.pdf

- Garcia, E., & Weiss, E., (2018). *Student absenteeism: Who misses school and how missing school matters for performance?* Economic Policy Institute. https://files.eric.ed.gov/fulltext/ED593361.pdf
- United States Department of Agriculture. (2017, July 18). *Eligibility manual for school meals: Determining and verifying eligibility,* 83-95. https://fns-prod.azureedge.us/sites/default/files/cn/SP36_CACFP15_SFSP11-2017a1.pdf

In the News / In the World of Practice:

- Lopez, B. & Lau, E. (2022, September 5). High-poverty schools struggle to earn Texas' highest rating. Some in the Rio Grande Valley break that trend. *The Texas Tribune.* https://www.texastribune.org/2022/09/05/rio-grande-valley-school-ratings/
- *The Los Angeles Times* Editorial Board (2019, December 27). Why do U.S. schoolchildren underperform academically compared with students in other countries? *The Los Angeles Times.* https://www.latimes.com/opinion/story/2019-12-27/why-do-u-s-schoolchildren-underperform-academically-compared-to-students-in-other-countries

Data Privacy and Compliance Considerations

The roster of which students qualify for FRLs is sensitive information and is generally restricted to personnel directly connected with the administration of the National School Lunch program. Any use of FRL data for other purposes, such as providing other services, requires informed parental consent (see Section 5 of the Eligibility Manual for School Meals, 2017). Apart from school cafeteria staff (typically cafeteria managers or leaders in a school's nutrition department), the only other staff who may have access to the FRL roster are those responsible for administering specific federal or state programs. The district must obtain consent to use the student's lunch status for other purposes (for example, school supplies or technology giveaways). In short, the information related to qualification for FRL is usable, but use categories must be satisfied, or additional consenting procedures must be followed, to ensure that the information is being used in alignment with privacy protections established by the Department of Agriculture (which administers the National School Lunch program).

"LEAs must avoid any policy or practice leading to the overt identification of children receiving free or reduced-price meal benefits" (USDA, 2017, p. 84). In addition, "Eligibility information cannot be made available to all school officials as a general practice." Sometimes teachers and other school personnel have a "need to know" about FRL status to carry out Federal programming. Certain tutoring programs can fall under this umbrella, but "access must be limited to a student's teachers who are directly responsible for the administration of a Federal education program or who provide a tutorial or other assistance under the educational program. Teachers, guidance counselors, principals, or other school officials who are not providing such assistance under the appropriate statutory or regulatory requirements cannot have access." Further, these individuals only have access to a student's eligibility status and are not privy to any additional information underlying the student's eligibility. Therefore, only those personnel providing the services should have access to the status of those children; educators and other personnel should not have information for students for whom they are not providing services and should

never have access to a comprehensive list of all students who qualify (USDA, 2017, p. 87). As a best practice, it is recommended that schools avoid sharing any non-aggregated data containing FRL status.

Maintaining the security of the roster of students who qualify for FRL is the responsibility of district and school leaders, who establish and maintain protocols for collecting, storing, and sharing confidential information. For schools with a well-developed Student Information System, a marker or tag may be visible in the SIS denoting students in various groupings (e.g., English language learners/emergent bilingual students, at-risk, race or ethnicity, sex, gifted programming, special education), and "economically disadvantaged" may be one of these, but the system must have a "masking or de-identification capacity to prevent unauthorized access to free and reduced-price eligibility status" (USDA, 2017, p. 87).

Sensitive information, particularly personally identifiable information–should only be shared with those individuals with a legitimate need to know. Guests of the school should not have information that in any way violates the privacy of the students, and this includes FRL identifiers. Leaders need to be careful to not only secure FRL rosters but also ensure the ways in which they communicate do not inadvertently allow others to connect the dots and unmask the FRL roster, in whole or in part.

Ethics and Norms

Only educators who serve students should be involved with academic planning and notifications for those students, especially when the services being provided inherently reveal that the student is not performing at expected levels. This area can be challenging to navigate: Leaders (and leadership teams) are often tasked with grouping students for services, particularly in connection with Response to Intervention or Multi-tiered Systems of Support. However, the groupings inherently reveal something about the other students' achievement measures to other students–by who is included in the group. While leaders cannot prohibit students from talking to their families about who else is participating in small group support, leaders can set the tone across campus by discussing the support in positive terms, pushing back on stigmas associated with support (after all, every human has both strengths and areas in need of development) and coaching teachers and tutors to adopt practices and language in line with an assets-based approach.

It's also important to recognize that, among the general public and certain educators, FRL status can itself give rise to stereotyping, particularly for those who associate poverty with underperformance, "laziness," or lack of ability. Explicit and implicit bias can lead educators to make assumptions about the causes of student underperformance or behaviors. It's important for leaders to distinguish between statistical associations (for example, that income tends to correlate with some markers of academic performance) and the idea that "data equals destiny." That is, poverty may be a substantial challenge, in that it limits resources known to be supportive of healthy growth and development (e.g., food security, access to reading materials and/or technology, stable housing), but the fact that a child is poor does not mean the child is destined for academic underperformance. Breaking these stereotypes by engaging teachers and staff in professional learning that helps them build resources for supporting students and for recognizing

talents, gifts, and assets that all students bring to the classroom, can help buffer or minimize the impact of deficit-based perspectives on student well-being and learning (Hammond, 2015; Theoharis, 2009).

One must consider the potential impact of stereotyping students based on economic status. Assuming students who receive free or reduced-priced meals need additional support (be it food or academic-related) or have behavior issues without considering other factors that may impact the student could prove harmful. When our biases drive decision-making, we often forget the child we are trying to help.

Leadership Practices & Data Use

One of the main tasks leaders must tackle is establishing a shared mission, vision, and direction for a school (Marzano et al., 2005). This requires work to establish trust with faculty, staff, students, families, and the community (Tschannen-Moran, 2014). If FRL lists are not kept strictly confidential, and families know that their placement on such a list will be known, trust will be negatively impacted between the families and the school. Even more importantly, breakdowns in practices to protect private information and confidentiality could deter families from completing FRL applications for their children, preventing them from getting the food (and related services) needed to succeed in school.

Leaders should also know their faculty and staff well enough to understand how they typically engage with students and the school community. Often, school personnel live in or near the attendance zones served by their students or shop or otherwise patronize businesses close to the school. They may also interact with students' families at faith-based, community, and commercial locations. Failure to keep the FRL list confidential can open families up to unfair scrutiny if personnel or other families question financial decisions or gossip about who they think should/should not apply for or qualify for FRL. This can also create tensions for students, or contribute to situations in which students are teased or harassed due to socioeconomic status. Therefore it is imperative that leaders not only practice appropriate data/information security protocols but that they also educate and impress upon faculty and staff the importance of such protocols.

Despite the importance of attending to various student groups in providing and monitoring academic outcomes, a district's hyperfocus on a particular group of students important to accountability ratings may be problematic (this is an open question for scenario users and may be debated). Do their actions suggest that students are to be prioritized *because* of their subgroup identification and the impact of that group on the school's "grade?" It's not that such a focus is unrealistic or even unimportant. Still, it is a focus that may spur the leadership team to prioritize students on the list, even at the expense of other students who could benefit from the same services. Data should be used to diagnose student needs and to support every student, not to game out which students "matter more" in the press for accountability ratings. Targeting and/or monitoring specific subgroups may feed a deficit perspective within the instructional team, as they could infer a perfect overlap between students on the FRL list with students who need additional support, be it academic, behavioral, or ancillary. For example, if the students included in the tutoring had been selected from among all those recommended for services based on

achievement scores and not the FRL meal list, the direct services provided would not overtly identify FRL students. In addition, the focus of support would be placed on those with academic needs based on achievement data points and not prioritized based on a targeted subgroup.

References and Resources

- Hammond, Z. 2015). Culturally responsive teaching and the brain: Promoting authentic engagement and rigor among culturally and linguistically diverse students. Corwin.
- Marzano, R. J., Water, T., & McNulty, B. A. (2005). School leadership that works: From research to results. ASCD/McREL.
- Park, J., Cotto, J., Waller Curtis, A., Klein, C. Reddy, A., Siegl, J, Sollberger, A., Triplett, J. & Vance, A. (2021, January 12). Student privacy communications toolkit: For schools & districts. Future of Privacy Forum. https://studentprivacycompass.org/resource/student-privacy-communications-toolkit-for-schools-districts/
- Snyder, T. & Musu-Gillette, L. (2015, April 15). Free or reduced price lunch: A proxy for poverty? NCES Blog. Institute of Education Science. https://nces.ed.gov/blogs/nces/post/free-or-reduced-price-lunch-a-proxy-for-poverty
- Theoharis, G. (2009). The school leaders our children deserve: Seven keys to equity, social justice, and school reform. Teachers College Press.
- Tschannen-Moran, M. (2014). Trust matters: Leadership for successful schools (The Leadership & Learning Center). Jossey-Bass.
- United States Department of Agriculture. (2017, July 18). Eligibility manual for school meals: Determining and verifying eligibility. https://fns-prod.azureedge.us/sites/default/files/cn/SP36_CACFP15_SFSP11-2017a1.pdf

Facilitator's Guide: Using Free /Reduced Lunch Qualification Status to Assign Student Support

Teaching Notes and Considerations for Scenario Facilitators:

This scenario allows users to work through decision-making related to data privacy/security practices, communication practices, and issues of asset vs. deficit-based perspectives, particularly as they might apply to students in poverty. Though school leaders are most familiar with FERPA, sensitive information related to student qualification for FRL is governed by the National School Lunch Act (NSLA) program, which is administered by the US Department of Agriculture (USDA). Privacy provisions are more restrictive under the NSLP program than FERPA, given the sensitivity of income-related data. This scenario, therefore, familiarizes users with privacy and security provisions associated with this the NSLA, which in many ways is central to attempts to serve all students equitably.

Extending Activities

- Assuming the leadership team at Ivy Middle School *wants* to target support for students in the "economically disadvantaged" category, develop a comprehensive selection and communication strategy that gets support to needed students without compromising student/family data privacy and avoids inviting stereotyping or stigmatizing of students. Include draft email or letter communications and phone and message scripts to use with family members, teachers, and the leadership team.
- Assuming the leadership team's strategy of prioritizing students in the "economically disadvantaged" category is inappropriate, work with a small group to develop an equity-oriented approach that your group can defend as making appropriate use of resources to meet student needs.
- Schools/ districts often offer additional support for economically disadvantaged students. These may include free lunch, breakfast, and/or after-school meals; free home internet/ hotspots; weekend backpack meals; personal hygiene products; tutoring; reduced fees for optional activities; etc.
    - How might a school/district ensure they are meeting the needs of their students without overtly identifying those who qualify for FRL?
    - What programs do you offer that are targeted at economically disadvantaged students? Could those programs lead to the identification of students who qualify for FRL? How might you restructure those programs to ensure student confidentiality?

Using Video to Increase Learning Opportunities

Learning Objectives

- Identify strategies and approaches that are well-positioned to meet the range of needs students may have when working in virtual learning settings.
- Describe benefits and risks afforded by virtual instruction specific to student privacy.
- Explain risks to student privacy involved in capturing video of a class and strategies for mitigating privacy risks when capturing, storing, and using video for educational purposes.
- Discuss strategies for inviting engagement in virtual learning settings while also mitigating risks to student privacy due to increased potential for persons with access to educational sessions.

Grady High School has been asked to explore a new approach to the traditional high school setting through a partnership with a neighboring high school and local college termed "One Dream, One Campus". The partnership would allow students to take classes offered by either high school and the college, and participate in community-based real-world learning and internships. Classes would be offered in different formats to allow students flexible schedules and increased options. Students may physically attend classes at any of the three campuses or online through synchronous or asynchronous classes. Since the school day hours will not allow for transportation between campuses, some classes will also be available through interactive video, accessible online or in a classroom setting at the other campuses.

To accomplish this programmatic flexibility, a common Learning Management System (LMS) would be adopted and teachers would be provided with software and equipment for interactive virtual classes. Several classrooms at each high school and the college would be set with similar equipment so students could attend the remote classes hosted by another campus. Some teachers would also use the software to teach fully online synchronous classes (no students in the host classroom). Select classes will be offered in the evening, most hosted by the college, but a few from the high schools. Since students may be in the community during class meeting times, all classes in the program would be recorded for later viewing.

Grady HS has formed a faculty and staff committee to vet this opportunity. They meet weekly to discuss the various opportunities and challenges of this new approach. This week's meeting focused on the video and recording aspects of the program.

The following is a summary of the discussion.

- Concerns about having to remember when to start/stop the recording led to questions about when the class should and should not be recorded:
    - Would the entire class period be recorded or just the parts with direct instruction?
    - What about when students ask questions or answer a teacher's questions?

- How do we handle recording small group discussions (through the software and in-person groups?)
- Can we record student presentations?
- What about teachers who have most or all of the students in person, do we record those classes as well?
- Do we need to record if all students are present?
- If I teach the same course for three sections, do I need to record all three, or just one?

> Considerations around student cameras:

- The other campuses will have cameras so we can see, and monitor, students in attendance. But what about students who are joining online? Will we require all students to be on camera? Will they be required to use a district laptop or can they use their personal device?
- For those joining from a location in the community or from home, should we be concerned about others being able to see and hear the class?
- Don't forget about the privacy of the student if they are joining from home. We want to be sure the camera doesn't catch something personal, inappropriate, or private.

> Questions about maintaining the recordings

- Where would we store the recordings, and how do we make them available for students?
- Do we only provide it to the students who request it, or do we post it somewhere for the entire class?
- How long do we keep the recordings?

Discussion Questions

> This scenario provides a small snapshot of questions and concerns that should be explored when considering video and recordings in the classroom. If a similar program were to be presented to your school, what additional questions, concerns, and considerations might you have?

> Take on the role of the principal facilitating the committee. How would you respond to the questions, considerations, and concerns posed?

> What guidelines need to be developed around video permissions when planning for virtual classes? How might the guidelines differ depending on the setting (in-person, virtual, hybrid)?

> If people other than the teacher appear in the video, does it matter if someone other than the students is able to view the video? In what ways might it be problematic or necessary

that siblings, parents, or others in a household may see the video? How might these issues be amplified if a class includes students in special situations (e.g., homeless, or other shelters, foster care situations)? Do the answers to these questions change when considering if the video is being viewed live or as a recording?

- What problems could emanate from students accessing videos of lessons showing other class participants (and possibly other members of their households)? How might these be mitigated?
- If Grady High School decided to engage in the "One Dream, One Campus" initiative, what permissions or communications around video and recording might you require and why?

From the Evidence Vault:

- Gill, J. (2022). Lessons learned from leading virtually. *Educational Leadership 79*(6), 54059.
- Rafalow, M. H. (2021). Digital equality requires more than access. *Phi Delta Kappan 102*(6), 26-29.
- Reich, J. (2021). Ed tech's failure during the pandemic, and what comes after. *Phi Delta Kappan 102*(6), 20-24.
- Stone, A. (2022, April 28). Understanding FERPA, CIPA and other K-12 student data privacy laws. *EdTech Focus on K12,* https://edtechmagazine.com/k12/article/2022/04/understanding-ferpa-cipa-and-other-k-12-student-data-privacy-laws-perfcon

In the News / In the World of Practice:

- Belsha, K., & Barnum, M. (2022, June 6). Sticking around: Most big districts will offer virtual learning this fall, a sign of pandemic's effect. *Chalkbeat.* https://www.chalkbeat.org/2022/6/6/23153483/big-school-districts-virtual-learning-fall-2022
- Blagg, K. (2021, February 26). How are states funding school districts in the wake of changing enrollments caused by COVID-19? *Urban Wire.* Urban Institute. https://www.urban.org/urban-wire/how-are-states-funding-school-districts-wake-changing-enrollments-caused-covid-19
- Ceres, P. (2022, Aug 3). Kids are back in classrooms and laptops are still spying on them. *Wired.* https://www.wired.com/story/student-monitoring-software-privacy-in-schools/

Data Privacy and Compliance Considerations

During COVID-19, when schools sought solutions for lesson delivery, the U.S. Department of Education (2020) clarified that schools did not violate FERPA simply by recording and making lessons available to students. They noted that an "education record" must be "directly related to a student" and "maintained by an educational agency or institution or by a party acting on behalf of the educational agency or institution" (2020, slide 24). Because the lesson itself is not "directly

related to a student" but to the delivery of content/development of knowledge and skills, it seems teachers would not be violating FERPA by recording classes to make them available for students otherwise unable to attend.

However, the issue at hand is not so simple. Whether recording classes for later viewing is okay includes other complicating factors. Leaders must consider:

- Who can access the videos and under what conditions/with what restrictions?
- How will videos be accessed (that is, via what platform), and does the platform/access meet security standards?
- How long will videos remain available, and where will they be stored between creation and (eventual) destruction? Does the method of storage meet IT requirements for security?
- Who will be captured in the videos (audibly or visually)?

Sometimes the answers to these questions will create other issues. For example, if no students are captured (audibly or visually) then, even if stored, the video does not become an "education record." However, if the video *does* capture students' voices or images (or perhaps comments, if a chat function is captured) and is stored in a way that is accessible, it is possible that an education record could be created. This could even be inadvertent: Consider a situation in which students are visible, but a student blurts out something that in some way shares personally identifiable information (PII) that is captured on the video. The teacher did not intend to capture or share PII, but the fact that the information now exists in a captured record, stored for use, and (if the teacher missed that PII was divulged), potentially viewed by other students and families. For more information on PII and other kinds of student data, see the *Student Privacy Primer* (Future of Privacy Forum, 2021).

Though the US Department of Education noted that recording and making lessons available to students who cannot attend virtual sessions does not in and of itself violate FERPA (2020), the same guidance noted that "As a best practice, educational agencies and institutions should discourage non-students from observing virtual classrooms in the event that PII from a student's education record is, in fact, disclosed in such virtual classrooms" (slide 20). Obviously, what can be viewed in a virtual classroom may ostensibly be captured in a recording of a virtual classroom, so educators who choose to record must be very mindful about how and what they are capturing, and who may be viewing. Many younger children will need assistance to navigate both virtual classrooms and recordings, so the expectation that "non-students" will not view recorded lessons seems unrealistic.

Leaders should remember that simply because they do not *expect* to use videos for unintended purposes, this does not mean a recording, once stored, may not be subpoenaed or otherwise duly requested. For example, if a teacher captures a video (with students present) for later viewing by students who were unable to attend the class session, and a behavior issue is captured on the video, a parent or administrator or another party may see the existence of the video as accessible evidence. A parent could see the video (even as they are assisting their child during a lesson) and use it to level criticisms or complaints, either through official channels or via unapproved posting of images/video segments.

To mitigate the odds of such risks, when possible, where videos are captured, they should not capture other students' images/voices, capture only the images/voices of students whose legal guardians have given permission for them to appear in videos for the purposes outlined (in permission/consenting/media release documents), or should angle a camera to minimize the ability of viewers to identify particular students.

In terms of data privacy compliance, if a teacher planned to simply post videos of herself teaching lessons to an online platform with viewing access restrictions, they would breach no privacy restrictions, as no student images/voices appear, and they would be making a voluntary choice to place their image and teaching skills into the video. The teacher might encounter other limitations in some venues, however, related to the copyright of materials (particularly regarding film or music elements she may desire to use in her lesson).

Ethics and Norms

Transparency is key in any leadership actions to garner and maintain the trust (of students, teachers, and families) (Grissom et al, 2021; Tschannen-Moran, 2014). Parents/legal guardians should be aware of any video capture where students are involved and the purposes for which video will be captured/used. Of course the simplest course of action would be to capture video without student images/voice; however, there may be pedagogical or content-related reasons that would necessitate the capture of student images/voices for the highest quality instructional video(s). In such cases, educators must work to ensure that PII are not disclosed in any way through the video and that appropriate permissions are secured from legal guardians for the use of their child's image/voice. These forms could be collected at a central time (registration, for example), but it is important that legal guardians know what they are signing (that is, that consents are not buried in "handbook acceptance notifications," for example) and that forms be adequately detailed (including what may be captured, where and for how long the content will be stored/used, for what purposes the content will be used, and by whom it may be accessed). The ethic of care to be used is: What would any reasonable parent (including the educator!) want to know about videos that captured their child and were then made available to others?

Related, leaders should regularly review any media use/release permissions, and make it easy for teachers to know for which students' particular media may be captured and shared. This is important in cases like the present (for video lesson purposes), but also because some parents may not want their child's image (even without a name) shared on a school or classroom website or social media page. Most districts have policies and many even have forms for this use, so it is important that leaders familiarize themselves with their own policies and take steps to ensure that everyone who works at their campus understands and abides by media use policies as well.

Another important ethical consideration specific to the creation of video lessons from actual virtual class sessions is that, if students' images and/or voices are captured, the educator risks capturing images/sounds of the students' homes, families, and personal lives that would not otherwise be shared in a classroom context. And further, rather than the sharing of such information being limited to other students, the broadcast of a video (even if restricted), can share this information with the families/friends of other students (or whoever is viewing the video).

Despite best efforts, it's not possible to ensure that only students and their caregivers involved in their education view video lessons, and it's all too easy for a student to use a cell phone or screen capture to grab a segment or image from a video of a virtual class and broadcast it to social media. Here, district policies can be helpful, if students are informed that they may not capture segments and share beyond the class. But in reality, that kind of policy may implement sanctions after the fact, but harm (in the form of embarrassment or sharing of private information) will have already been done by the time any sanctions are in place. This is why it's critical for educators to consider what needs to be captured, to best serve students educationally and how that information can be captured without unnecessarily putting other students' privacy at risk.

Leadership Practices & Data Use

It is commendable that Grady High School took the time to understand the needs of the students and staff considerations to determine if the "One Dream, One Campus" program would be a good fit for their school. Effective principals support the development of productive, collaborative problem-solving cultures (Grissom et al., 2021; Starratt, 2004). Professional Learning Communities (PLCs) are a perfect place for such work to occur (though PLCs can sometimes get bogged down in information-sharing, becoming little more than glorified meetings). PLCs were originally designed as laboratories of problem-solving, where teams of educators posed problems of practice and engaged in inquiry and evidence use to improve practice. That is precisely what the school has encouraged during the committee meetings. Scenario users might consider where in the workday leaders in their respective contexts have created space for such problem-sharing and solution-seeking (both as a whole-school and for professional teacher teams/PLCs). They might also consider how the school's process reflects the team-based approaches to data-rich problem-solving described in evidence-rich processes (Boudett et al. 2014; Safir & Dugan, 2021; Schildkamp et al., 2018).

In this case, it would be important to engage with district IT personnel. When creating, storing, and using educator-created resources that use or contain school-owned materials, resources, or facilities, it is important for the educator to use district-approved equipment and software and to post only to district-approved platforms. Schools should provide guidance on where and how to store these resources to ensure their privacy and protect them from breaches or otherwise unwanted access.

Any time student data, including images, are captured and posted, there is a risk of data breach. If the videos are captured, stored, and accessed through district-licensed products that have appropriate security measures, these risks can be reduced, though not eliminated. While knowing and abiding by district policies and procedures for data creation and storage is a responsibility of any educator, in the fast-paced effort to get instruction to students, data creation and storage policies may not be ever-present on teachers' radar. Furthermore, teachers may not have comprehensive knowledge of what constitutes an "educational record." It is a responsibility of school leaders to engage in ongoing professional learning that helps teachers and staff understand the importance of these responsibilities and to provide them with adequate connections and resources to help them do their jobs well and in alignment with privacy and data security requirements.

Finally, in terms of general privacy practices, it's important to recognize that the best case scenario may not be the most practical approach. For example, it requires a significant amount of time for a teacher to record a separate "video only" version of instruction. Although this would eliminate the risk of capturing student images, voices or PII, one must consider the impact on the teacher and the building culture. Consideration should be given to the teacher's time to capture, edit and manage recordings, as well as the effort to create lessons that are adapted to the hybrid or virtual learning environment.

As a "lesson only" version does not include responses to various students, it will likely be shorter and more navigable for students who access the material asynchronously. At the same time, it could generate more questions via email or other communication that require additional teacher time in responding to student (or family helper) queries. Leaders are responsible for "creating and sustaining a healthy organizational environment for teaching and learning for all students and teachers" (Starratt, 2004, p. 63). In light of this ethical responsibility, school leaders must consider the totality of what they are asking/expecting of teachers and provide adequate resources to make the work feasible, in order to achieve quality virtual instruction.

References and Resources

- Boudett, K. P., City, E.A., & Murnane, R.J. (2014). Data wise: A step-by-step guide to using assessment results to improve teaching and learning (Revised and expanded edition). Harvard Education Press.
- Figure of Privacy Forum. Student Privacy Compass. https://studentprivacycompass.org/resources/?audience=educators
- Grissom, J.A., Egalite, A.J., & Lindsay, C.A. (2021). How principals affect students and schools: A systematic synthesis of two decades of research. The Wallace foundation. Available at https://www.wallacefoundation.org/knowledge-center/pages/how-principals-affect-students-and-schools-a-systematic-synthesis-of-two-decades-of-research.aspx
- Kaufmann, M. (2020, April 6). U.S. Department of Education clarifies that video recording virtual lessons and making them available to students does not violate FERPA and provides other advice on FERPA compliance in the age of virtual learning. JD Supra. https://www.jdsupra.com/legalnews/u-s-department-of-education-clarifies-41746/
- National Forum on Education Statistics (2021). Forum guide to attendance, participation, and engagement data in virtual and hybrid learning models (NFES2021058). U.S. Department of Education. Washington, CDL National Center for Education Statistics. https://nces.ed.gov/pubs2021/NFES2021058.pdf
- Park, J., Cotto, J., Waller Curtis, A., Klein, C. Reddy, A., Siegl, J, Sollberger, A., Triplett, J. & Vance, A. (2021, January 12). Student privacy communications toolkit: For schools & districts. Future of Privacy Forum. https://studentprivacycompass.org/resource/student-privacy-communications-toolkit-for-schools-districts/
- Starratt, R. J. (2004). Ethical leadership. Jossey-Bass.
- Future of Privacy Forum (2021, October 5) Student privacy primer.

https://studentprivacycompass.org/resource/student-privacy-primer/

- Tschannen-Moran, M. (2014). Trust matters: Leadership for successful schools (The Leadership & Learning Center). Jossey-Bass.
- United States Department of Education (2020, March 30). FERPA & virtual learning during COVID-19. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPAandVirtualLearning.pdf
- Waughn, C. (2020). Rethinking video mandates in online classrooms: Privacy and equity considerations and alternative engagement methods. https://studentprivacycompass.org/videomandates/

Facilitator's Guide: Using Video to Increase Learning Opportunities

Teaching Notes and Considerations for Scenario Facilitators:

Scenario users find no simple answers in this case but have the opportunity to brainstorm paths forward toward a goal of creating and sustaining learning structures and practices that take into account a range of student and family needs. In doing so, they will also consider aspects of data privacy, ethics, and leadership. While not all applications of data use, ethics, and privacy will be covered by these teaching notes, below we point out several areas that facilitators may choose to emphasize or further explore as they lead groups in learning with the scenario.

Finally, we acknowledge that virtual instruction became prominent during the response to COVID-19. Much of the guidance that has been issued around student privacy, virtual instruction, and recordings was released during that time. However, scenario users should keep in mind that online instruction provided learning opportunities to students prior to the pandemic and will continue to do so as educational philosophies evolve.

Extending Activities

- Examine policies, requirements, and practices in your school/district context. Then, develop a plan for virtual instruction (synchronous, asynchronous, or blended) that meets instructional and funding requirements without contributing to inequities in learning opportunities.
- Consider your entire student population and the accommodations and services offered to students. Some may have 504 plans or IEPs, others may have services provided under another program or tier intervention.
    - What process, practices, equipment, and strategies might need to be put in place in order to provide similar accommodations in a virtual setting?
    - How would you ensure accommodations and indirect services (such as you would have in a co-teaching setting) for students with 504 Plans or IEPs while maintaining the privacy and dignity of those students?
    - What precautions are needed to ensure the privacy and dignity of students with visible disabilities during virtual learning?
- Discuss the issues involved in recording a class or a lesson. How would that work? Who should be in the video? Who should not? What are the risks and advantages? Investigate possible platforms and software options/apps for capturing and storing instructional videos.
- Investigate the possibility of virtual instruction in your context. What challenges would need to be addressed to provide equitable and excellent instruction in a situation where virtual instruction was needed?

Working with Researchers in Schools

Learning Objectives

- Understand the university and/or district-level Institutional Research Board (IRB) approval requirements and the relationship to FERPA.
- Understand the restrictions around conversations that contain student information.
- Delineate procedures school leaders might use to cooperate with approved research studies/researchers while also communicating boundaries for data/information sharing between school personnel and research personnel.
- Identify and generate approaches to address potential conflicts of interest when research is conducted by persons who are also school/district employees.

McArthur School District is located in a region that is also home to three community colleges and four universities. These institutions partner with the district to provide graduate programs to district staff at an affordable rate with a flexible schedule. The close proximity of the institutions, in addition to the partnership programs, results in frequent requests by graduate students to conduct research within the district. Sometimes these persons are researchers associated with one of the area higher education institutions; sometimes they are district employees aiming to conduct research as part of the requirements of their respective graduate programs.

This district has a policy and well-established process for research conducted within the district. Each research request is reviewed by the Assistant Superintendent of Leadership, Evaluation, and Continuous Improvement, Dr. Winters. The approval process requires prospective researchers to complete a district-level application-to-research form and to affix the university's IRB approval (or contingent approval, if the university process requires district agreement for a final determination of approval). Dr. Winters reviews applications in concert with the district's Director of Technology and three other district employees who hold doctoral degrees and have experience in conducting research. Two parent representatives and a community member also sit on the committee, which reviews requests to research monthly. During the most recent meeting, the committee reviewed three studies.

Study 1

The district released an invitation to conduct a study on the three high schools' efforts to improve mathematics instruction. The selected researcher will work with teachers and instructional coaches to explore practices that support student success. Dr. Cooke, a well-known university researcher, responded to the invitation. As part of his response to the invitation, Dr. Cooke stated that his work will result in both reports for the district as well as publications and presentations related to mathematics education, His proposal includes a formal written agreement that adheres to the requirements of a contract under FERPA's studies exception, including the collection, use, storage, and disposal of student personally identifying information. As part of the agreement, Dr. Cooke stated he would collect student demographic information, work samples, assessment results, classroom observations, student attendance, and discipline referrals.

The committee reviewed the provided statement of work and written agreement and debated the request for data. Some committee members expressed concern over the request for attendance and discipline data and questioned if it was necessary for the evaluation of teaching methods. Other members wondered if some of the data would meet the same need in either de-identified or aggregate form. Further discussion focused on limitations that should be included regarding the use of the data for publications and presentations.

Study 2

Dr. Jackson is a professor at a local university in the College of Education. Before she transitioned into higher education, Dr. Jackson was a high school chemistry teacher and assistant principal, so she easily relates to the teachers and staff in the building. She is an active parent volunteer at one of the district elementary buildings. Since she is in the building frequently, there are times that Dr. Jackson overhears conversations regarding student performance.

Dr. Jackson has recently received a grant to study the current climate and culture in the school community. She submitted a proposal to include the district in this study, specifically assessing a student's sense of belonging. In her proposal, she requests to conduct student surveys about belonging. Although she does not wish to collect student names, she does request that survey results be tied to a unique identifier that can be cross-referenced with the following individual information: age, grade, race, ethnicity, grades by subject, assessment data, number of discipline referrals, and number of nurse visits. She includes the approval for the research by the University's IRB.

The committee discusses the intersection of Dr. Jackson's School Official's designation under FERPA, her access to students, and the research being conducted. One committee member questions if this proposal is research or would qualify under the FERPA Studies exception. Another member asked about the IRB approval requirements and if the IRB considers the District's federal and state compliance requirements, including FERPA and potentially PPRA, when providing IRB approval.

Study 3

The third proposal is from Ms. Winters, an assistant principal at one of the district's high schools. As a doctoral student, Ms. Winters is beginning her work on her dissertation. She is seeking permission from the district to research the implementation of Professional Learning Communities (PLCs) and their impact on student performance. She hopes to use a questionnaire, observations of PLC meetings, educator interviews, and student assessment data to assess the effectiveness of the building's departmental PLCs.

The committee discusses how she might ethically approach the work from the dual roles of school leader and researcher. They work through what data she can access, how, and for what purposes within the research. Since she has student-level data access as an assistant principal, they wonder what safeguards need to be put into place to ensure the privacy of student data as this will be considered research and will not utilize the Studies exception.

Discussion Questions

- If you were a committee member, how would you respond to the questions and comments in each proposal?
    - Study 1: Some committee members expressed concern over the request for attendance and discipline data and questioned if it was necessary in the evaluation of teaching methods. Other members wondered if some of the data would meet the same need in either de-identified or aggregate form. Further discussion focused on limitations that should be included regarding the use of the data for publications and presentations.
    - Study 2: The committee discusses the intersection of Dr. Jackson's role as a volunteer, her resulting access to students, and the research being conducted. One committee member questions if this proposal is research or would qualify under the FERPA Studies exception, or if parental consent would be required. Another member asked about the IRB approval requirements and if the IRB considers federal compliance when providing approval, including FERPA and potentially PPRA.
    - Study 3: The committee discusses how she might ethically approach the work from the dual roles of the school leader and researcher. They work through what data she can access, how, and for what purposes within the research. Since she has student-level data access as an assistant principal, they wonder what safeguards need to be put into place to ensure the privacy of student data as this will be considered research and will not utilize the Studies exception.
- What other considerations might the committee need to discuss?

From the Evidence Vault:

- Attai, L. (2019). Protective measures: In today's environment, school ed-tech initiatives are only as cool as the data-privacy safeguards that undergird them. *Educational Leadership 76*(5), 60-63.
- Barnes, K. (2015). The challenge of data privacy. *Educational Leadership 73*(3), 40-44.
- CrashCourse (2019). Henrietta Lacks, The Tuskegee Experiment, and Ethical Data Collection: Crash Course Statistics #12. https://www.yout-ube.com/watch?v=CzNANZnoiRs

In the News / In the World of Practice:

- Privacy Technical Assistance Center (PTAC) (2014, April). FERPA exceptions-summary. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20Exceptions_HANDOUT_portrait.pdf
- The University of Chicago Department of Computer Science (2023, February 21). UChicago and NYU research team finds edtech tools could pose privacy risks for students. https://cs.uchicago.edu/news/uchicago-and-nyu-research-team-finds-edtech-tools-could-

pose-privacy-risks-for-students/

Data Privacy and Compliance Considerations

A few data privacy and compliance issues stand out in the scenarios noted. The first issue is appropriate review and approval for any study in the school context. Researchers who are affiliated with a university (and some who are affiliated with research associations) typically submit their planned research (including focus/purpose, design, instrumentation, procedures, and approaches for protecting the rights and privacy of human participants) to an Institutional Review Board (IRB) for approval. As part of this submission, researchers specify how data will be collected, protected, stored, and disposed of. If data will be stored for use for other purposes, that must be made clear in the study application and disclosed to potential participants.

It is important for district leaders to understand the primary function of the IRB is to review ethical and safety considerations for research involving human subjects. As stipulated in Title 45 CFR 46, Basic HHS Policy for Protection of Human Research Subjects, approval for research is based on the following criteria: risks to subjects are minimized, risks are reasonable in relation to anticipated benefits, selection of subjects is equitable, informed consent is sought and appropriately documented if required, adequate monitoring of data to ensure the safety of subjects, adequate provisions to protect the privacy of subjects, and additional safeguards for vulnerable subjects. Several categories of education research may be exempt as set forth under § 46.104 Exempt research. This includes "[r]esearch, conducted in established or commonly accepted educational settings, that specifically involves normal educational practices that are not likely to adversely impact students' opportunity to learn required educational content or the assessment of educators who provide instruction. This includes most research on regular and special education instructional strategies, and research on the effectiveness of or the comparison among instructional techniques, curricula, or classroom management methods."

Additional research that is common to the educational setting is defined as exempt. Although the research may be exempt from needing IRB approval by federal policy, some universities may choose to require approval. Additionally, the review is often limited to the ethical nature of the research and the researcher's handling of the data. IRBs are not required to review and ensure compliance with laws and regulations that govern the subject of the research. Therefore, it is the district's responsibility to ensure that they maintain FERPA, PPRA, IDEA, and other applicable state, local, and federal regulations.

Even if researchers can collect interesting data beyond the bounds of the approved study, they should confine themselves to the study design (or, if necessary, submit amendments to the IRB and the district before collecting new data). Data outside of the bounds of the approved study are considered out of bounds and should not be made available to the researcher even if the educators willingly share those data. In the case of a staff member conducting research at the behest of the district, what is collected, how, from whom, and when should all be governed by the written agreement that must accompany the "studies exception" to FERPA (see PTAC, 2014).

In the case of volunteers, the district would be well-served to remind teachers about privacy protections and caution them about discussing specific situations-even sans names–with persons

who do not have legitimate educational interests or in spaces where persons without legitimate educational interests can overhear. Anytime an individual's role moves from a volunteer to a researcher, it is a good time for the district to discuss potential “insider/outsider”/role issues.

In all cases, information shared with researchers is either done so in cooperation with a request for de-identified data or with appropriate consenting mechanisms (when not a study undertaken by or on behalf of a district) or is governed by written agreements to adhere to FERPA’s studies exception or FERPA’s audit and evaluation exception (the two exceptions that would allow a researcher to access student data without parental consent). These agreements are required to specify the purpose, scope, and duration of the study and what information the researcher will be given. There may also be additional requirements and limitations for research in state student privacy laws.

Ethics and Norms

There are times when approving an external research study is impractical (for example, when a study design unduly burdens teachers, particularly during already-hectic times of the year). At the same time, if schools regularly decline opportunities to cooperate or collaborate with external researchers, there would be little opportunity to deepen or expand research upon which “evidence-based practices” are established. Further, a common complaint is that “ivory tower” researchers don’t always understand the realities of schools; however, if the school doors are routinely closed to researchers, this divide will only be exacerbated.

Districts may have to make a challenging decision to approve, deny, or modify research conducted by someone familiar with the student subjects. This may be an employee, volunteer, or possibly even a consultant/vendor. Access to students in the educational setting as a “School Official” does not give the individual legitimate interest in data for research purposes. That access is only permitted under the FERPA studies exception or with direct parental consent. Regardless, if the research or study explores sensitive information covered under PPRA, direct parental consent would be required. In the scenario above, it is highly possible that research on climate/culture and a student’s sense of belonging would meet the criteria of parental consent under PPRA. In the case of Dr. Jackson, the parent volunteer, careful consideration is needed to explore and define the intersection and separation of the volunteer/vendor role and the researcher role. This is especially important when the individual is designated as a “School Official” with “legitimate educational interest” in student data. Each role, volunteer/researcher, and resulting access to data must be well defined to mitigate ethical and legal challenges.

The case of Ms. Winters is a common situation for leaders obtaining Master's or Doctoral degrees. The rule to live by for student-practitioner-researchers is: If you were not currently employed in your position, would you have access to the data you intend to use? If the answer is “no” (and the answer is often “no”), then it’s critical to think through how the role of an employee (“insider”) intersects with that of a researcher (“outsider”) and to not only seek approval (typically from an IRB as well as the district) but to build in safeguards to protect data as well as to ensure that participants in the study do not feel coerced to participate. It’s important to remember that even the most altruistic school leaders still have perceived authority of position, so others “invited” to participate in research by leaders may experience (unintended) coercion. This is, in

part, why establishing a clear study design and thinking through potential research complications–particularly in complex settings like schools–is a critical component of such studies.

School leaders, staff, and teachers must be aware of situations where they may be considered "researchers," such as completing projects (including treatises, capstone projects, and/or dissertations) related to graduate program work. When educators are in these situations, they should be careful not to capture, store, use, or share data about students that could identify individual students unless proper parental consents are in place. Being in possession of data is not sufficient, ethically, to justify using those data for research/graduate school purposes. When researchers want to collect data or information about students, they need to articulate--with approval from the district and/or campus--a plan for what they will collect, when, and from whom (see National Forum on Education Statistics, 2013, and PTAC, 2015a, b).

Leadership Practices & Data Use

There is a difference between "research" or "evaluation" that happens outside of the normal course of school improvement processes (often involving or led by external parties, or by practitioner-scholars like Ms. Winters) and more common data-informed internal improvement processes or evaluation/research activities undertaken at the behest of district leaders. Whether designed as "action research," "continuous improvement," "improvement science," or "DDDM," these processes involve practitioners establishing questions of interest, collecting and analyzing data to inform the next steps, implementing possible interventions, and assessing results.

Several guides effectively describe these internally-focused, improvement-oriented processes (e.g., Bernhardt, 2017; Boudett et al., 2014; Hendricks, 2016; Hinnant-Crawford, 2020; Mandinach & Jackson, 2012; Mintrop, 2016; Schildkamp et al., 2018). Because having a school-driven, improvement-focused design does not automatically exempt those involved from seeking approvals for some disclosures or from abiding by established privacy requirements (e.g., FERPA, district policies, and practices), it is important for educators to be able to distinguish between regular-course-of-business improvement efforts that involve data and "research or evaluation" efforts that involve data for purposes beyond district-initiated school improvement. Finally, it's important for educators to recognize that, even in school improvement situations, identifiable data are often unnecessary; aggregate or de-identified data may be perfectly sufficient for the purposes established. Where aggregate or de-identified data can be used, those are the data that should be used (see Future of Privacy Forum, 2021; PTAC 2013).

School leaders should work in concert with district administration to construct and clarify any issues pertaining to any request to research or research agreement. They should consult with district administrators and/or policy to determine whether and how parents should be notified that a study is taking place, even when parental consent is not required. The best practice is transparent practice: Parents/guardians need to be aware of ongoing studies or situations in which their child(ren)'s data may be used for research and improvement purposes.

Beyond building their own knowledge base around research procedures, ethics, and data privacy, it is incumbent upon school leaders to make their faculty and staff aware of where and

when they discuss student information, especially if there are visitors, parents, researchers, or other outsiders present during such discussions. Even if a researcher has an approved IRB and contract under the FERPA Studies exception, some data should not be discussed with that researcher because they may be beyond the study's data collection boundaries as outlined in the contract.

While we would expect that external researchers would follow their ethical guidelines and abide strictly by their proposed study designs, the ultimate responsibility for complying with FERPA falls to the school leader. It is vital that schools utilizing the studies exception to FERPA have appropriate safeguards in place to ensure that no more information is shared than allowed under the applicable exception and agreement that they appropriately protect data used in other approved studies as per district policies, any consenting requirements, and approved study parameters.

References and Resources

- Bernhardt, V.L., (2017). Measuring what we do in schools: How to know if what we are doing is making a difference. ASCD/
- Boudett, K. P., City, E.A., & Murnane, R. J. (2014). Data Wise, Revised and expanded edition: A step-by-step guide to using assessment results to improve teaching and learning. Harvard Education Press.
- Future of Privacy Forum (2021, October 5) Student privacy primer. (2021, October 5). https://studentprivacycompass.org/resource/student-privacy-primer/
- Henricks, C. (2017). Improving schools through action research: A reflective practice approach. Pearson.
- Hinnant-Crawford, B. (2020). Improvement science in education: A primer. Myers Education Press, LLC.
- Mandinach, E. B. & Jackson, S.S. (2012). Transforming teaching and learning through data-driven decision making. Corwin.
- Mintrop, R. (2016). Design-based school improvement: A practical guide for education leaders. Harvard Education Press.
- National Institutes of Health (NIH). (2016). Guiding principles for ethical research. https://www.nih.gov/health-information/nih-clinical-research-trials-you/guiding-principles-ethical-research
- Park, J., Cotto, J., Waller Curtis, A., Klein, C. Reddy, A., Siegl, J, Sollberger, A., Triplett, J. & Vance, A. (2021, January 12). Student privacy communications toolkit: For schools & districts. Future of Privacy Forum. https://studentprivacycompass.org/resource/student-privacy-communications-toolkit-for-schools-districts/
- Privacy Technical Assistance Center (PTAC) (2014, April). FERPA exceptions-summary. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20Exceptions_HANDOUT_portrait.pdf

- Privacy Technical Assistance Center (PTAC) (2013, May). Data de-identification: An overview of basic terms. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/data_deidentification_terms.pdf
- Schildkamp, K., Handelzaltz, A., Poortman, C. L, Leusink, H. Meerdink, M. Smit, M., Ebbeler, J., & Hubers, M.D. (2018). The Data Team(™) procedure:A systematic approach to school improvement. Springer.
- Siegl, J. (2022, April). Mythbusters–Student privacy edition: Common myths, misinformation and misunderstandings. Presentation included on the program of the Interoperability & Privacy Symposium. Future of Privacy Forum.
- U.S. Department of Health and Human Services Office for Human Research Protections (OHRP) (2020, June). Human Subject Regulations Decision Charts: 2018 Requirements. https://www.hhs.gov/ohrp/regulations-and-policy/decision-charts-2018/index.html#c13
- National Archives Code of Federal Regulations (2023, June). 45 CFR 46.1. https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-A/part-46/subpart-A?toc=1

Facilitator's Guide: Working with Researchers in Schools

Teaching Notes and Considerations for Scenario Facilitators:

The scenarios described in this case involve various ways practitioners may commonly engage with research or researchers. As schooling aims to be "evidence-based," it is important for practitioners to engage with researchers when possible. How that happens, though, is dependent on practical, ethical, and privacy-related factors that should be considered by all parties.

The three research situations here differ in a few ways, including whether the study is rooted in a district-initiated request and the positionality of the researcher(s). Though these three scenarios do not cover all potentialities that attach to research in schools, they do provide a jumping-off point for exploring intersections of policies, practices, privacy protections, ethical considerations, and collaborations that accompany the various kinds of inquiry projects that occur in PK-12 school contexts.

Extending Activities

- Expand upon Study #2 with the parent volunteer, as well as Study #3 with the school staff member. Districts may have researchers who have direct access to students under a "School Official" designation with "legitimate educational interest." What ethical and legal compliance concerns may result from the dual role? Under what conditions (type of research, research topic, extent of research, form of information/data collection) might districts consider allowing or not allowing school officials to research students with whom they have direct access? How might districts mitigate these concerns and potential challenges from real, or perceived, misuse of FERPA-protected information?
- Review your district's policies and procedures with regard to research studies. What has to be prepared and submitted, and to whom? Who decides whether a study can be conducted, and are there further procedures in place that guide communication of the researcher with faculty, staff, parents, or students? What role does the campus principal play in the approval or oversight of the study?
- Brainstorm reasons school leaders should consider supporting or hosting research studies, when possible. Brainstorm reasons that might require leaders to decline to support or host studies. Reflect on factors that would lead you to support a study on your campus/in your district. What factors would lead you to decline support/hosting? Discuss your responses with a small group and debrief.
- Imagine that a school or district employee, like Ms. Winters, is considering conducting a research study in their own school/district. Using a T-Chart, delineate the kinds of data the person would have access to–absent any formal research agreement–as a "researcher" and in their "current role." Do the same for the responsibilities to others (students, faculty, staff, parents, communities) that would be attached to each role. Discuss with a small group how a person functioning in both roles–simultaneously–can navigate legal and ethical issues with transparency and integrity.
- Craft a brief "entry plan" for situations when studies are approved to take place on or in

conjunction with personnel on your campus. How will you inform teachers/staff about the study? What information should you share, with whom, and how? How will you meet the researcher/research team and what questions should you ask (if any)?


FUTURE OF
PRIVACY
FORUM