TECHNOLOGY

These scenarios include the use of an application or other piece of technology.

Topics: Technology/Virtual Learning

Accidental Sharing of a Tab

Ms. Emma is using a video conferencing tool to conduct a virtual lesson to her science class. Like many people during the pandemic, she has a number of different websites and tabs open on her browser. One tab contains an email she was drafting to a colleague about a student, Olivia, that contains personal information and student performance data. Inadvertently, Ms. Emma switches from tab to tab and the email is visible on the screen for the entire class to see.

Questions for discussion:

- What precautions should Ms. Emma take to protect documents and windows on her computer while teaching class?
- What risk did Ms. Emma take by not closing extraneous tabs?

USER'S GUIDE: Accidental Sharing of a Tab

Here's how we see it:

- Extreme care around technology must be taken so that no information is inadvertently shown to students.
- Ms. Emma should use fresh windows with no tabs when sharing her screen to others to minimize the risk of sharing student data or other tabs that should not be shared.
- Ms. Emma should seek guidance from administration on how to proceed as the inadvertent disclosure of information could potentially be problematic under FERPA, especially depending on the sensitivity of the email content.

For further discussion:

- Does it make a difference if the content of the email is positive or negative?

Unintended consequences:

- Other students now have seen that Emma is communicating about Olivia to other educators. They could taunt Olivia and impact her self-esteem if the data and information were negative.
- If the data were positive, the students could still unnecessarily tease Olivia because she could be considered the teacher's pet.
- Depending on the information that was shared, this could be a potential violation of FERPA.

Topics: Student Data/Technology

Accidentally Disclosing Student's Grade

Mr. Cane is teaching high school band in a virtual environment. He uses the SmartMusic platform to share music scores with students, have them record parts of their practice, and to provide two-way feedback. SmartMusic is approved for use by his school. The platform is very helpful with connecting with students, therefore, he also uses SmartMusic when working with youth through his own private trumpet classes, completely separate from his school classes. While he is returning comments and scores a school student has received for class, he accidentally sends the comments and a copy of the score to a private student he coaches, Jennifer, with the same name. The parents of the private trumpet student, Jennifer, are very upset about the comments.

Questions for discussion:

- How should Mr. Cane respond?
- What could Mr. Cane have done to prevent this problem?

USER'S GUIDE: Accidentally Disclosing Student's Grade

Here's how we see it:

- The student's whose score was shared had their privacy violated by sharing their education record. This is problematic from a FERPA perspective and will most likely be seen as a violation since there was most likely no parental consent. Mr. Cane should consult administration to discuss this accidental disclosure of student education records.
- Mr. Cane should use separate accounts and ideally different computers for school and private students.
- School licensed software should only be used for school projects.
- Mr. Cane must also now ensure that these comments are deleted from Jennifer's device and are not shared with anyone else.

For further discussion:

- What are the privacy concerns for students?
- Should teachers keep personal and private accounts for software platforms?

Unintended consequences:

- The private student who received the negative comments was harmed because the feedback was unwarranted as it was not for her score.
- The student and their family whose scores and comments were shared can feel a breach of trust and confidentiality. Jennifer may know the student and therefore can lead to social harm, such as stigmatization and bullying.

Topics: Communication/Technology

App Mistranslation

During a virtual English as a Second Language class, Mr. Sendo works with two students Rafat and Niema. They are both new immigrants whose native language is Arabic but Rafat is from Morocco and Niema is from Egypt. Mr. Sendo is sharing his screen and using Google translate. Mr. Sendo asks the students to describe their country. The students use Google Translate to help them formulate their sentences in their own language, translate the sentence into English and then read it to the class. Niema writes: “Egypt is a beautiful country, but Morocco does not have a good smell”. Rafat becomes extremely upset and starts yelling at Niema in Arabic. Niema looks confused and Mr. Sendo realizes there may have been a mistranslation.

Questions for discussion:

- What should Mr. Sendo’s next steps be?
- How can Mr. Sendo rebuild the relationship between the students in a virtual setting?

USER'S GUIDE: App Mistranslation

Here's how we see it:

- Tools such as Google Translate are powerful tools for bridging language barriers and divides. They also come with the risk of bad translations, misinterpretation, and cross-cultural insults.
- Teachers should make sure translation apps are approved by their school and verify the accuracy of translations to help prevent social harm.
- Mr. Sendo should address the insults with both students and their parents/caretakers.

For further discussion:

- How would this situation be different if it was in a physical classroom?
- What could Mr. Sendo do to prevent this type of situation from happening in other classes?

Unintended consequences:

- Online tools such as Google Translate are useful but come with concerns about social harm and safety when statements are mistranslated, used for harm, or to insult.

Topic: Technology

Breach of App Used by Students

Coach Kittles explores ways to keep his basketball players engaged and focused on skill building during the off season. He has each athlete download the HomeCourt app onto their phones that lets them work on their dribbling skills in a video game format. The players set up their phone camera so they can see themselves then the app shoots video of them responding to movement and dribbling cues. The players are excited about the app because they can compete with each other online and push each other to improve their skills. One day, Coach Kittles and all the players receive a notification from the app that some personal data was stolen via a breach.

Questions for discussion:

- Would the scenario change if you knew if the app was approved by the athletic department or the school district?
- What responsibilities does Coach Kittles have?

USER'S GUIDE: Breach of App Used by Students

Here's how we see it:

- Teachers and coaches must make sure any apps used by students are approved and verified by the school or school district, whether for academic or athletic use. This allows the district/school to ensure the app complies with privacy laws and so they can take appropriate action if a breach occurs.
- Coach Kittles should immediately reach out to administration so they are aware and so they can address the situation. Coach Kittles should also seek guidance from administration on how to communicate this incident and how it is being handled to families as quickly as possible.

For further discussion:

- How can coaches protect student data privacy from being compromised when they use approved edtech tools?
- What responsibilities do coaches have to protect student data privacy?
- What happens when an athletic coach or teacher uses an unapproved app? Where do the responsibilities lie?

Unintended consequences:

- There is always a risk of an app being breached, putting student data at risk. This risk is more severe when educators/coaches ask students to use an app that has not yet been vetted by the school or district.

Topics: Communication/Technology

CC'ing Parent Email Addresses

Sydney Middle School has a Gifted and Talented program. Ms. Anderson writes an email to all the parents (and caretakers) of the program. When sending the email, she puts all the parent emails on the same line, with none of them as a blind carbon copy (BCC). Parents can therefore see other parents' email addresses — and thus, possibly identify other students in the Gifted and Talented program.

Questions for discussion:

- Does the school need to put parents' email addresses in a BCC?
- What are the ramifications of parents finding out who the other Gifted and Talented students are?

USER'S GUIDE: CC'ing Parent Email Addresses

Here's how we see it:

- The school should not allow these addresses to be visible to other parents. This is not necessarily a violation of privacy laws because it is directory information in most states, but it could be if, for instance, certain parents have opted out of disclosing email addresses.
- The issue is more about best practice - in exposing email addresses, the school has unintentionally identified the Gifted and Talented status of many students. Regardless of any privacy laws, the school is ethically bound to do a better job protecting caregivers' email addresses.

For further discussion:

- Gifted and Talented status is positive, so why does it matter if people know?
- Is the answer different for a Gifted and Talented identification than for Special Education identification?
- Would it be okay for parents to be able to communicate with one another based on the school email?

Unintended consequences:

- The inadvertent disclosure of email addresses can lead to unwanted emails, spam, solicitations, or even hate mail. Even though there might be a close knit group of parents for this class, the protection of their email addresses is proper practice. If one parent wants the email of another parent, then there can be an agreed upon exchange of information, but it should not come from the teacher or the school.
- There is the possibility that parents can glean which students are not in the program, leading to stigmatization.

Topics: Student Data/Technology

Choosing College Major

Over the next few weeks, Ms. Cole's 11th-grade students have individual meetings with the guidance counselor, Mr. Freeman, to discuss what major they would like to pursue in higher education. One of her students, Quinton, comes back from his meeting visibly upset. Ms. Cole finds a time to talk with Quinton and learns that Mr. Freeman recommended this student pursue business instead of biology, dashing his hopes of becoming a biology professor. Ms. Cole decides to speak with the guidance counselor to learn more.

Mr. Freeman tells Ms. Cole that the school has recently acquired a new analytics-based advising tool to determine what career path is best for each student. This tool creates real-time, formative, and predictive assessments based on demonstrated interest, demographics, performance, and historical individual and institutional data points. The counselor lets Ms. Cole know that, based on the advising tool's assessment, Quinton is shown to be at risk of dropping out of higher ed if he were to pursue his major of choice, while he has a greater chance of success with the major Mr. Freeman has recommended.

Questions for discussion:

- How should Ms. Cole respond to this explanation? Should she support the recommendation made by Mr. Freeman and this new tool?
- What conversation should Ms. Cole have with Quinton? Should she have a conversation with his family as well?

USER'S GUIDE: Choosing College Major

Here's how we see it:

- Advising tools like those used by Mr. Freeman can provide valuable insight into a student's skills, strengths, and interests. However, it is important to remember that data is prone to bias, and any insight generated from these tools should be the start of a conversation, not the end. An important decision such as choosing a college major should not be decided by a black box of information with limited transparency on what data is being used to inform that decision and how this data is collected. Quinton, and his family, should have agency to challenge the tool's recommendation and make sure the decision is also informed by assessments from Quinton's teachers and with Quinton's interests and desires. Ms. Cole should ask how Mr. Freeman recommended the specific major to Quinton and what additional data, beyond the tool, he may have incorporated into the process.
- Quinton and his family should be a part of the conversation to craft his future options, not merely recipients of a recommendation. Quinton's teachers, family, and Quinton himself should work together to create a plan to help Quinton work towards his goals.

For further discussion:

- What are potential advantages and harms that come from using predictive analytics data?
- If you were in Ms. Cole's or Mr. Freeman's position, what other data would you incorporate into your decision making? How would you position/frame that decision to Quinton? His family?

Unintended consequences:

- Predictive assessment tools can lead to unfair and biased outcomes. There is severe potential harm to Quinton's future, and other students' futures, if the recommendation of this tool is taken without any other factors or considerations.

Topic: Technology

Computer Accidental Data Exposure

Mr. Huey is a social studies teacher at Buddy High School. He has a classroom computer where he keeps student records, and he has another computer at home where he also keeps student records. Mr. Huey invites some colleagues, Ms. Sally, Mr. Winston, and Mrs. Naomi, over to his home to do some collaborative work on a project. The colleagues sit down to discuss the project. As Mr. Huey is on the computer and showing Ms. Sally some documents and websites, Ms. Sally notices some student work products, such as quiz grades, that do not pertain to the collaborative work.

Questions for discussion:

- Is it a problem that Ms. Sally has seen the unrelated student work?

USER'S GUIDE: Computer Accidental Data Exposure

Here's how we see it:

- Computers where student data and personally identifiable information should be protected and locked down no matter where they are and to whom they belong. School communities are small, and it is possible that a teacher's child or others could snoop if computers are unlocked to find out information about their friends.
- This inadvertent disclosure could possibly be a privacy violation if Ms. Sally did not have a legitimate educational interest in seeing the data; however, since all teachers are bound not to disclose student information, unless Ms. Sally rediscloses it, it is unlikely to violate law but could still harm the student (breach of trust, bias by Ms. Sally to the student, etc.).
- Regardless, Mr. Huey should take measures to protect any data on his computer, such as the data that Ms. Sally saw.

For further discussion:

- How might Mr. Huey better protect student information on his home computer?

Unintended consequences:

- It is possible that there might be some data that even colleagues should not see that could skew how they potentially see students after viewing the data.

Topic: Technology

Facial Recognition

A large urban high school, Willie High School, installed facial recognition software to be used for campus security in lieu of identification cards. The software is based on artificial intelligence algorithms that have been tested primarily on white faces. The software is known to be less accurate when it comes to other racial groups. It is also particularly bad at recognizing and distinguishing children's faces. However, the system was already purchased with grant money, was very expensive, and it will supposedly be more secure than having students and faculty show ID cards each time they come into school. Since the system was launched, there have been problems. There is always a teacher standing by at the beginning of school to observe students as they walk through the scanner. On one day, Mr. Carter observes several students of color, Bailey, Rico, Jackson, and Jen, being misidentified and stopped by security.

Questions for discussion:

- What are the ethical ramifications of using such a system?
- What are the data privacy implications?

USER'S GUIDE: Facial Recognition

Here's how we see it:

- Research has shown that the algorithms that underlie facial recognitions are indeed less accurate for various racial groups and women.
- Continued profiling of certain groups of students eventually will become problematic, as it can result in disciplinary recourse and effect permanent records.
- One possible solution, though up to school administration and district staff, is to allow students to opt-out of the system and allow them to stick with ID cards.

For further discussion:

- Discuss some of the concerns about using the technology when there are issues with accuracy, especially differential accuracy.

Unintended consequences:

- Because the software is flawed, the inaccuracies will disproportionately target students of color.

Topic: Technology

Heart Rate Monitor on Smartwatch

The Conwell High School Physical Education program purchased a class set of smartwatches with heart rate monitors. The students use them to monitor their heart rate during class to determine if they are working in their target heart rate zone for 30 minutes per class. At the end of class, the smartwatches sync via Bluetooth to the students' account on a school approved app for tracking fitness. Being in your target heart rate zone for 30 minutes per class is counted as 50 percent of the students' grade. The target heart rate zone is a standard metric for all students based on their age. The heart rate data syncs automatically with the student grade book. Jimmy is an athlete on a travel soccer and basketball team. Every period he goes for a run with friends and often does a High Intensity Interval workout. Despite all this activity he often has a difficult time getting his heart rate in the target zone. Ms. Padder receives a complaint from Jimmy's parent, Ms. Ziggy, because his grade is a D minus, primarily because of his heart rate data.

Questions for discussion:

- What are the data issues in this scenario?
- How can Ms. Padder address Ms. Ziggy's and Jimmy's concerns?

USER'S GUIDE: Heart Rate Monitor on Smartwatch

Here's how we see it:

- The generic algorithm in the smartwatch app that bases heart rate zones solely on age is flawed as it does not take into consideration highly trained athletes such as Jimmy whose resting heart rate is normally lower and on the end of the spectrum for students with a high resting heart rate.
- The department could explore options with the current company or research other apps that do take into account resting heart rate of the student.
- Ms. Padder should teach all students how their resting heart rate impacts their target heart rate and have them make manual modifications to their target zone.
- The settings that automatically transmit the heart data to the grade book should be changed until a system or app is implemented that takes into account variations in resting heart rate.

For further discussion:

- What other data and personal privacy concerns can you think of concerning student health data?

Unintended consequences:

- Students may receive unfair grades if influential variables that affect the smartwatch data are not taken into account.

Topic: Technology

Learning Management System Data Dashboard

To aid teachers for another semester of remote learning, Mr. Williams and his colleagues are shown the different tools and data that are made available in their learning management system (LMS). Teachers are able to see student scores from online assignments and quizzes, but also LMS activity data, such as how long students spend in the different learning units, how many times they access quizzes, and at what times of the day they log in.

After completing his classes' first semester learning unit, Mr. Williams accesses the data dashboard, which includes student scores from the assignments and quizzes and the relevant LMS activity data. He sees a general trend that students who spent less time logged into the unit did poorer on the unit's final exam. Mr. Williams decides that for the next unit, he will use the dashboard to check how many minutes students spend in the unit every week to identify which students might be at risk of failing.

Questions for discussion:

- What do you think about how Mr. Williams will use this activity and log in data?
- Should Mr. Williams communicate to students and families about what LMS activity data they are collecting and how they plan to use it?

USER'S GUIDE: Learning Management System Data Dashboard

Here's how we see it:

- It is understandable for districts, schools, and teachers to want to use timely data to provide immediate feedback and support, as opposed to the end of the course or unit, especially in an unfamiliar learning environment. With that being said, it is a best practice to communicate to families and students about all the types of information that are collected, especially data that parents may not consider. Communication with families and students about how LMS data will be used builds transparency in how teachers monitor students and provides an opportunity for families to ask questions.

For further discussion:

- What factors could affect minutes spent in an online unit? How could these factors be influenced during a pandemic and social unrest, especially for students from marginalized communities who are learning from home or elsewhere?

Untended consequences:

- Minutes spent on an activity is only a proxy in identifying which students are at risk of failing. Minutes spent on an activity can be an indicator of a number of other factors. If Mr. Williams limits who he offers help to only students with low minutes spent on a unit, this could leave out other students who need help.

Topic: Technology

Parent-Recommended Educational App

The parents (and caretakers) of several different students from Ms. Kumar's class reach out to her to recommend the same educational app. The parents tell Ms. Kumar that friends of theirs with kids at another school have been using this app and love it. Ms. Kumar is familiar with this school district and knows they uphold similar strong privacy protections before allowing teachers to use any edtech tools.

Questions for discussion:

- Is it okay for Ms. Kumar to move on this recommendation from parents? Why or why not?

USER'S GUIDE: Parent-Recommended Educational App

Here's how we see it:

- Ms. Kumar should not act on parent recommendations alone and must proceed through her district's process for vetting and approving any apps before using them in her classroom. Before even taking this step, Ms. Kumar should first determine if this is a tool she wants to use. Ms. Kumar should consider how it fits into her instructional practice and if there is another tool they are already currently using and that has already been approved, with a similar function and purpose.

Unintended consequences:

- The app could violate student privacy laws or district and school policy if it does not undergo the appropriate vetting process.

Plagiarism Detected by Software

The Harley School District has put in place software that can detect plagiarism in students' work products. Mr. Levi gives an essay assignment to his ninth grade English class and runs his students' essays through the software. Two students' papers are flagged as questionable. Mr. Levi approaches Lucas and Dante.

Questions for discussion:

- How should Mr. Levi approach suspected students?
- Does Mr. Levi have to inform the students that he is using the detection software?
- What actions should Mr. Levi take?

USER'S GUIDE: Plagiarism Detected by Software

Here's how we see it:

- Plagiarism is serious and should definitely be addressed.
- A concern first is to determine if Lucas and Dante understand what they did is wrong. The situation may be one of not understanding the concept. In that case, it is a teachable moment.
- The software output should be combined with Mr. Levi's knowledge of the students. It may not be 100 percent accurate, but it can point to irregularities.

For further discussion:

- What happens if the software output differs from what Mr. Levi suspects?
- What if the software flags language that Mr. Levi thought was cited and used appropriately?

Unintended consequences:

- A student could be wrongly accused of plagiarism. Incidents of plagiarism on a student's permanent record can result in loss of opportunity, including college rejections or loss of scholarship.

Topics: Student Data/Technology

Posting Student Videos on YouTube

Ms. Kowalski is putting together a virtual mini theater performance with her middle school theater class. She has each student record a short video of them performing their lines of the play and send them to her. Once she has all the videos, she edits them together and posts them on her school district YouTube channel as a public video to make it easier for students and parents to find. She also shares it with parents/caretakers and staff members via email. The next day, she receives an angry email from Jacob's mother saying she was very upset that his likeness was on YouTube. Jacob's mother says she had not consented to have him appear in video format. Ms. Kowalski reviews the school's video and photo release data and realizes that Jacob's mother is correct, she had only agreed to photographic representations.

Questions for discussion:

- What should Ms. Kowalski have done to prevent this problem?
- How can she remedy a solution?
- Would it be different if it was Ms. Kowalski's personal YouTube account rather than the school's account?

USER'S GUIDE: Posting Student Videos on YouTube

Here's how we see it:

- When using student likeness in any public setting teachers must verify what permissions parents have given for each student.
- Ms. Kowalski should immediately take the video down to edit out the video of Jacob. Ms. Kowalski should also seek guidance from administration to amend the breach of trust and harm that was done.
- The harm would have been worse had it been from Ms. Kowalski's personal account.
- The main point of harm is the platform that the video was shared on. Anything posted on YouTube, be it privacy or unlisted, would still be considered public. There would be different implications if the video had been posted to an internal district drive or learning management system, which has much stronger access limitations.

For further discussion:

- Would sharing a student likeness within a physical class for a project have different requirements?
- If Ms. Kowalski had posted the video as Unlisted or Private on her YouTube channel would this change the issues?

Unintended consequences:

- There is potential for student likeness posted on YouTube to be shared infinitely, even if it is a school account, especially if the settings are public. Anyone can watch these public videos, it can be reshared on social media accounts, and people can comment on the video.
- There is potential for legal and personal harm to Jacob as his parents did not authorize the use of his image on video.

Topics: Technology/Virtual Learning

Proctoring Software

Ms. Hughes is giving a test to her students. This test has to be done under standardized and secure conditions. But the test is virtual this year so extra procedures and precautions have been introduced by the district including a proctoring software. Students take the test at home and Ms. Hughes hopes for the best. Ms. Hughes is concerned that her students might try and game the test. The proctoring software indicates potential cheating by some of the students.

Questions for discussion:

- What actions should Ms. Hughes take?
- Is observing the students while taking the test in any way a violation of their privacy?

USER'S GUIDE: Proctoring Software

Here's how we see it:

- Ms. Hughes should assess why the software is indicating possible cheating and discuss with the students to see if there is a rational explanation. Ms. Hughes may also want to discuss these incidents with the appropriate administrators.
- A key difference between how test proctoring would occur in person versus online, is that the software could be reporting false positives. In an in-person situation, the teacher would be accountable to noticing instances of cheating. Additionally, with students learning from home, there could be a number of factors triggering the proctoring software, especially if students do not have a private, quiet place to take their test.

For further discussion:

- What should happen if the software and Ms. Hughes' observations did not agree?

Unintended consequences:

- The proctoring software can lead to false positives. Furthermore, just having the software in place can add increased stress and anxiety to students while taking the test.

Topics: Technology/Virtual Learning

Recording Virtual Class on Personal Device

Mrs. Rayne is teaching a virtual class that requires students to produce some visual displays of their work. Mrs. Rayne is really concerned that she will forget which student has produced which product, so she decides to record the class session using another device, not the recording feature of the district-approved video conferencing tool. Mrs. Rayne pulls out her mobile device and records each student as they present their work. Mrs. Rayne does not tell the students she is recording their presentations.

Questions for discussion:

- Has Mrs. Rayne done anything wrong by recording the students and their work? If so, how?
- Would it make any difference if Mrs. Rayne had used the district-approved video conferencing tool to record rather than her mobile device?

USER'S GUIDE: Recording Virtual Class on Personal Device

Here's how we see it:

- Mrs. Rayne should check with the district to ensure that she is not violating any policies by recording her students. Mrs. Rayne should also determine if her district permits or requires recording of lessons. No matter district policy, it is not good practice to record students on personal mobile devices. Many times, mobile devices do not have the same privacy protections as district devices and platforms. And these student recordings could easily be accidentally shared with unauthorized people when stored on a personal mobile device.
- Mrs. Rayne should also take into account that this recording may be FERPA protected, and as a result parents/caretakers would have the right to access this recording.
- Students may be able to exercise their rights to say that they are not comfortable being recorded and opt out, depending on the district policy.

For further discussion:

- Is it necessary and appropriate for Mrs. Rayne to inform her students that she is recording the class?
- Most video-conferencing tools show when a session is being recorded. Is that sufficient notification for the students in lieu of telling them?

Unintended consequences:

- Storage of these recordings on personal, mobile devices heightens the risk of it being shared with unauthorized persons because its main purpose is for personal use. The mobile device could be stolen, someone could look through the gallery and find the recordings, or the recordings could be accidentally shared in a text message.
- Students may have had difficulty with the project, so having their presentation recorded could add increased pressure and look bad to peers who could make fun of them for a bad work product. Thus, the recording of the activity could lead to low self-esteem for students whose work gets criticized.

Topics: Classroom Practices/Technology/Virtual Learning

Recording Virtual Classes

Mrs. Garcia will use a district-approved video conferencing tool to conduct her social studies class during distance learning. From student and family communication, Mrs. Garcia knows that it will be difficult for all of her students to join the class every day and so decides to record her classes to offer asynchronous learning and more equitable access for her students.

Questions for discussion:

- Is it okay for Mrs. Garcia to record the virtual classes?
- Is there anything Mrs. Garcia should be cautious of?

USER'S GUIDE: Recording Virtual Classes

Here's how we see it:

- It is laudable that Mrs. Garcia took the time to understand the needs of her students during distance learning and used their needs to inform her decision to record her classes. With regard to whether Mrs. Garcia is allowed to record her classes, she should look to school or district guidance in this legally gray area.
- If her school and district say it is permissible to record classes, Mrs. Garcia should only use district-approved video conferencing platforms when conducting and recording classes. Mrs. Garcia should also seek school or district guidance on where to store these recordings, to ensure these recordings are privacy protected from breaches or otherwise unwanted access.
- Mrs. Garcia should also carefully consider how long she will retain these recordings. They should not be retained indefinitely and not retained longer than needed.
- Mrs. Garcia should also communicate her recording practices to students and families so they are aware and so they have the opportunity to raise any questions or concerns.
- Mrs. Garcia should consider which parts of classes should be recorded. For example, students may feel much differently about lectures being recorded versus student-led classroom discussions.

For further discussion:

- What communication should Mrs. Garcia provide to her students regarding recording of the classes?
- What are some concerns students and families may have in learning the classes will be recorded?

Unintended consequences:

- If not properly stored, these recordings can be hacked into and leaked.
- Students may feel a breach of trust with Mrs. Garcia and a breach of privacy, especially if they are not made aware in advance of being recorded during live instruction.
- Recording student discussion can have chilling effects—meaning students are less willing to participate and voice their opinions because they know they are being recorded.

Topics: Technology/Virtual Learning

Screen Sharing

Students in Ms. Gordon's middle school Multimedia Arts class are sharing their self-portrait projects during an online critique on a video conferencing platform. The project involves manipulating their self-portrait in photoshop. Each student takes turns sharing their screen, while the other students follow a structured critique process. Jonah shares his screen to show his manipulated self-portrait. In the image his face is overlaid with multiple images of penises.

Questions for discussion:

- How should Ms. Gordon respond?
- What options does she have to mitigate the harm to the other students?
- What if Jonah did not mean to share this manipulated self-portrait?

USER'S GUIDE: Screen Sharing

Here's how we see it:

- Teachers should be intentional with the videoconferencing platform settings and the ability for students to share their screen. Allowing students to screenshare can foster collaboration and increase engagement, but there is also the risk of students sharing something inappropriate, be it accidental or not. Expectations should be set on what is allowable to be shared and caution advised to students on how to use the sharing screen feature.
- Instead of allowing students to share their own screens, Ms. Gordon could share student work from her own screen after pre-screening the work.
- The most immediate step Ms. Gordon should take is to stop Jonah's screen sharing.

For further discussion:

- What are the privacy risks for the students?
- What are the privacy concerns for Jonah?
- How would the scenario be different in a physical classroom?

Unintended consequences:

- Social harm and age-appropriate content are the biggest concerns. The other students were exposed to images that were not age-appropriate without their parent's consent.

Topics: Technology/Virtual Learning

Sending Kids into Breakout Rooms

While teaching science online, Mr. Riley has students working in small groups to develop an experiment. In class he sends each small group into breakout rooms. The breakout rooms are difficult to monitor as the platform does not allow recording of the rooms and students have unlimited access to screen sharing and chat functions. When students come back from working in the breakout room Mr. Riley receives a direct message from Jacob saying that Kimberly shared her screen during the breakout room and showed a pornographic website. Jacob felt very uncomfortable and said he was going to talk to his parents.

Questions for discussion:

- What are the next steps for Mr. Riley?
- Who should Mr. Riley talk to?
- What are the safety and privacy implications for Jacob and Kimberly?

USER'S GUIDE: Sending Kids into Breakout Rooms

Here's how we see it:

- Online breakout rooms for students without monitoring present a challenge for teachers for classroom management, student safety, and student privacy. Mr. Riley must develop a plan for monitoring breakout rooms in a systematic manner, reteach classroom expectations for breakout rooms, and contact the parents/caretakers of both students to explain what happened and discuss the next steps. Mr. Riley should also seek out guidance from administration to determine if and what disciplinary action may take place.
- The data privacy concerns are minimal in this case study. On the other hand, the personal privacy concerns regarding the possibility of students being exposed to unwanted content in an unmonitored chat room are more complex.

For further discussion:

- How can Mr. Riley incorporate breakout rooms into his lessons while protecting student safety and privacy?
- Are online breakout rooms the same as small group discussions in classrooms?
- What if this had happened in a classroom with a student showing pornographic images on a phone in a small group? What are the differences?

Unintended consequences:

- Breakout rooms without direct adult supervision have the potential to expose students to speech, images, and language that would have more protection in a monitored situation.

Shared Document

Mr. Clive is teaching English at Brandy High School. He is using Google Docs as a platform for his students to collaborate on writing assignments. Students work together on essays and other group projects. It is usually a team effort. One group consists of Camille, Daisy, Tonya, Lee, and Otto. A document thread has begun and students add text and comments. Mr. Clive notices that one of the students, Otto, has made some really nasty comments. There is evidence of Otto bullying the other students in the group.

Questions for discussion:

- What should Mr. Clive do, given that he has observed this behavior?
- Would Mr. Clive's actions differ if Camille, one of the students, brings the harassment to his attention, rather than having seen it first-hand?

USER'S GUIDE: Shared Document

Here's how we see it:

- Addressing this bullying incident and Otto's actions is absolutely in Mr. Clive's purview, as this is happening on a school document for a school purpose. Mr. Clive should address the comments with Otto and also ensure expectations for the different functionalities of different apps and tools have been covered with the class.
- When using newer apps and tools (that have been vetted and approved by the school/district), teachers should be sure to understand all the different possible functionalities to discuss expectations with students regarding their use.

For further discussion:

- Would Mr. Clive's options be any different if he observed the harassment first-hand rather than in the Google Doc?

Unintended consequences:

- Students may abuse different aspects of newer apps and tools and this abuse can happen unsupervised if a teacher is not aware of these features.

Topic: Technology

Signing up for an Educational App

Mrs. Hart found a math app on the list of district-approved tools that she wants her students to use. She asks all students to sign up for the app. One of her students has difficulty signing up, so she walks this particular student through the process. As she is helping the student sign up, she notices all the information the app is asking the student to enter: first and last name, grade, age, home address, email, profile picture, a list of favorite things such as color and food, and a username and password.

Questions for discussion:

- Should Mrs. Hart have the students fill out all of this information? Is there any information students shouldn't fill out? If so, which ones?

USER'S GUIDE: Signing up for an Educational App

Here's how we see it:

- It is possible that not all of the information the app is asking for is necessary or required for the main purpose or functionality Mrs. Hart intends to use it for. Username and password will most likely be required, but the other information might be optional, such as profile picture and home address. Since this is a district-approved app, we can assume that the district has vetted the app, determined that it complies with privacy laws, and that students are okay to input all information, even when optional. But it is best practice for teachers to minimize the amount of student data collected by apps, even when district-approved. For example, some students may feel uncomfortable uploading a picture of themselves or not have a home address because they are in transition. Therefore Mrs. Hart can give them clarity on what information is mandatory to access the tool versus what information students can choose whether to input.

For further discussion:

- What instruction should teachers provide to students signing up for a new app or service and inserting information?

Unintended consequences:

- Students may feel uncomfortable submitting certain types of information and doing so may lead to social harm.

Topics: Technology/Virtual Learning

Students Sharing Videos with Teacher

Mr. Randall is teaching virtual Physical Education and is looking for ways to increase student accountability for completing the fitness challenges he sets for his students. He is concerned the results being reported by his students are not accurate. For the student push up challenge he assigns students to use FlipGrid to document the challenge. FlipGrid is an approved app in the Madison School District. It is a video discussion and message platform that allows teachers to pose questions and prompts using video that students comment on or respond to using video. He is careful with his FlipGrid settings in that he sets it so the videos only come to him to protect his students' privacy and he is the only one who can comment on student performance through the videos. Most of his students post their push up challenge videos to document doing as many pushups as possible in 1 minute. Mr. Randall sends back video coaching of their technique. Later in the week, Mr. Randall receives an angry email from Mrs. Stanley, the parent of his student Emily, saying that she is very concerned that a male teacher is watching videos of her daughter doing pushups in skimpy workout outfits. Mrs. Stanley is extremely angry in the email and feels the use of the videos is not educationally appropriate.

Questions for discussion:

- What are ways for Mr. Randall to respond to Mrs. Stanley?
- Does the gender of the teacher impact the situation?
- What are the privacy implications of using video sharing applications?
- If the FlipGrid is not approved for use by the school district does that change the discussion?

USER'S GUIDE: Students Sharing Videos with Teacher

Here's how we see it:

- The app is approved for use by the Madison School District which allows for Mr. Randall to use the app with his students. Mr. Randall was not sharing an education record, the video, with anyone. Mr. Randall should work with the parent to address the concern, and possibly include an administrator.
- Mr. Randall should also consider the importance of proactive communication and transparency with parents/caregivers. A notice from Mr. Randall to all families about this new practice he was adopting—students sharing videos of their workouts—would most likely have prevented this response. Parents can feel a breach of trust without proactive communication. Proactive communication also grants a space for families to give feedback and input and for Mr. Randall to improve the practice and make it more comfortable for everyone.

For further discussion:

- What are ways Mr. Randall could have protected students' concerns about video sharing?

Unintended consequences:

- Sharing videos is a powerful educational tool both for in person and virtual learning but it raises concerns about student personal privacy and comfort with video sharing. Teachers should be thoughtful about its use and implementation. Teachers, such as Mr. Randall, must explicitly explain the value and need for it to students and parents through proactive communication.

Topic: Technology

Teacher Laptop Crash

Ms. Dory is a teacher who keeps her gradebook on her personal laptop. Ms. Dory does this because it is more convenient than using the desktop in her classroom—this way, she can work on grades at home or a coffee shop. One day, the laptop crashes while she is doing her grades. Ms. Dory takes it to a computer repair person, Mr. Zie, that she trusts and has used before. Mr. Zie is able to fix the laptop and restore the grades she was working on.

Questions for discussion:

- Is there a problem with taking this laptop to an external repair person?
- Would it be different if Mr. Zie was the district technology repair person instead of an independent repair person?
- Can teachers keep student personally identifiable information (PII) on personal equipment?

USER'S GUIDE: Teacher Laptop Crash

Here's how we see it:

- The main problem is that by taking the laptop to Mr. Zie, Ms. Dory has exposed student names, grades, and any other information to Mr. Zie. It doesn't matter if Mr. Zie actually sees it or not—the opportunity is there.
- A district technology repair person is a much better choice because they are generally authorized by the school to fix computers that have student personal information on them. However, the teacher should ask administrators who they should take the laptop to for repair.

For further discussion:

- Is there a difference in keeping PII on a personal laptop or a personal smartphone?
- What issues does it raise that Ms. Dory works on grades outside the school? Is her home any different than a public coffee shop?

Unintended consequences:

- An individual without authorization to view the grades may have seen them. One does not know if Mr. Zie might speak about the grades, know some of the students, or even make modifications to the gradebook if he happens to have a connection with one of the students.

Topic: Technology

Teacher Viewing Student Data During Class

A teacher at Sebastian High School, Ms. Mia, has given her students time to do homework in class. She takes advantage of that time to explore student performance on the assessment system on the computer. Through this system, Ms. Mia is able to view student assessment histories and insert new grades. As the students do their homework, they sometimes come to Ms. Mia's desk to ask her a question. Ms. Mia does not make any attempt to shield her screen or lock her computer when a student comes to the desk.

Questions for discussion:

- Should Ms. Mia shield her screen or lock her computer? Why or why not?

USER'S GUIDE: Teacher Viewing Student Data During Class

Here's how we see it:

- Ms. Mia should make a reasonable effort to ensure that students cannot see her work when they come to her desk. Some of the assessment histories or personal demographic information might be Personally Identifiable Information (PII) which should not be viewed by unauthorized individuals (e.g., students) pursuant to FERPA. Even if some data is not PII, Ms. Mia is ethically bound to ensure that students do not see each other's data.
- Ms. Mia can solve this in many ways. For instance, she might install a screen filter that makes it hard to see what is on the computer unless you are directly in front of it, she might lock the computer, or she might simply minimize the program window when the students come to her desk.

For further discussion:

- Would it matter if Ms. Mia was working on information from another class? Especially if it were another section of the course where the students did not know each other?
- What other options does Ms. Mia have to protect the PII when she is talking with the students?

Unintended consequences:

- It is possible that a student can see data or information about other students to which they should not have access. Such viewing could lead to bullying, stigmatizing, taunting, etc. It is best to ensure that students cannot see any data other than their own.
- This could also lead to a potential violation of FERPA.

Topics: Professional Duties/Technology/Virtual Learning

Tracking Attendance During Remote Learning

The Shea School District instituted new policies in the wake of the pandemic to collect attendance data. All educators have been struggling to obtain accurate data about student attendance while conducting virtual instruction. Mr. Bartlett and Ms. Tatum have been worried about getting accurate counts of their students. Some students have their cameras on and others do not. Some students may be "in attendance" for the entire class time, whereas others may go missing at various points in time. The school has advised teachers to use student login data from the learning management system (LMS) to track attendance. Yet there is no real way for teachers like Mr. Bartlett and Ms. Tatum to know if it is actually the specific students who are logged into the LMS and not someone else.

Questions for discussion:

- Can a LMS provide accurate attendance data?
- Is the use of time in the LMS not only a valid indicator of attendance but also an appropriate use of the data?
- Are there privacy concerns about using LMS data or on-camera data for attendance indicators?

USER'S GUIDE: Tracking Attendance During Remote Learning

Here's how we see it:

- Having accurate attendance data is a part of compliance and accountability data for a district. Getting it right is important.
- The district is making an assumption that the student on the LMS is the student of record. This assumption has the potential of being inaccurate as it is possible that when students first log into their LMS, they remain logged in for a long period of time. There also needs to be protections so that students are only able to log into their own account in the LMS.
- Furthermore, an LMS may not track student logins from phone or tablet devices. This would mean students using these types of devices would have absences falsely reported.

For further discussion:

- What if someone else is on the LMS and not the student?
- How can the teacher ensure or determine if it is the real student who is logged into the LMS?
- What are the ramifications if it is the wrong student?

Unintended consequences:

- Potential harm can occur if a student's attendance is not accurately recorded. In this situation, using LMS login data to track attendance will disproportionately harm students who are using a table or phone device.
- There is potential harm for the school and district as well for inaccurate attendance data.
- The validity of attendance as a data element is in question and could be impactful for district funding if recorded inaccurately.

Topics: Technology/Virtual Learning

Unknown Virtual Class Attendee

Forrest Schools has moved online and decided to use a video conferencing platform to conduct virtual classes. To mitigate the possibility of unauthorized access into these virtual classes, the Forrest School has tried to password protect entry into classrooms. Yet, one day, Mr. Ares notices someone other than his students in the Zoom meeting room. Entry was done using a phone number so that is all Mr. Ares can see. He asks who is in the room but gets no answer.

Questions for discussion:

- What action should Mr. Ares take?
- Is this a violation of student privacy?

USER'S GUIDE: Unknown Virtual Class Attendee

Here's how we see it:

- Mr. Ares should be aware of the setting and capabilities of the video conferencing platform he is using. Most likely, Mr. Ares should be able to boot out the unknown attendee. Mr. Ares should also set the expectation that if students must join from a phone number, which can assist during technical difficulties, to communicate in advance with the teacher when possible and introduce oneself when joining the call.
- School or district policy will determine whether or not this intrusion is considered a violation. Mr. Ares should therefore seek out this policy and guidance from administration in determining what are the appropriate next steps to take.
- There are reasons that schools lock down video conferencing meetings to protect the sanctity of the classroom to inadvertent intrusions from people who should not be there. Such intrusions can potentially put students at risk.

For further discussion:

- What kinds of assistance should the school provide Mr. Ares?
- Is there potential harm for anyone other than the students and teacher to have access to the secure room?

Unintended consequences:

- The potential harm is that an uninvited and therefore unauthorized guest or interloper would be able to learn and have access to student information, including who is in the class and, if student cameras are on, information on their living situation. Also, consider an extreme situation where an interloper has a restraining order to stay away from one of the students. Schools have a legal obligation to uphold these restraining orders.
- The interloper could potentially disrupt instruction with inappropriate language, images, or content in the virtual classroom.

Topic: Technology

Working at Home on Grades

Mrs. Kimberly is a teacher at the Petals School and is grading at home one evening on her district-issued laptop. Each time she gets up, she locks the screen—and only she knows the password. As Mrs. Kimberly is working, it is just her family in the apartment—her husband, her 6-year-old, and her 4-year-old.

Questions for discussion:

- Does Mrs. Kimberly need to lock the screen every time she's away from the computer? Why or why not?

USER'S GUIDE: Working at Home on Grades

Here's how we see it:

- Absolutely, Mrs. Kimberly needs to lock the screen every time she gets up. Grades when correlated with a student are considered Personally Identifiable Information (PII) that is part of an education record, and PII in education records must be secured at all times that the authorized user is not with them. Besides this, it is important for Mrs. Kimberly's career and safety that she is always able to say that she followed these procedures to the letter of the law.

For further discussion:

- If Mrs. Kimberly's husband does not care what the grades are, and the kids are too young to understand them, what would it matter if she left her computer unlocked?
- What if Mrs. Kimberly's children were older? What if they were also students at Petals School? Would either of those changes to the scenario change your answer on whether Mrs. Kimberly should lock the screen every time she's away from the computer?
- What other things could go wrong if she leaves it unlocked?
    - For example, maybe one of her kids starts hitting keys and accidentally changes grades — and nobody notices.
    - An email inadvertently gets sent with a grade file.
- What are other ways to secure Mrs. Kimberly's device, aside from locking it?

Unintended consequences:

- Although it is unlikely that toddlers can understand what they see on the computer screen, they can inadvertently make changes to the gradebook without Mrs. Kimberly's knowledge, only to be discovered later (or not). It is also unlikely that Mrs. Kimberly's husband will do anything to the computer but protecting it and keeping it locked down will prevent any accidental modifications to files that potentially could change students' grades, and it will also prevent him from having access to information he should not have access to.