iKeepSafe™ Generation Safe™

360 Self Assessment Tool

PRINTABLE VERSION

Provided by SWGfL

360 degree safe

iKeepSafe Generation Safe
360 Self Assessment Tool

GENERATION SAFE™ 360 SELF ASSESSMENT: PRINTABLE VERSION

Contents

Introduction

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT skills, not only to maximize their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment.

There is a large body of evidence that recognizes the benefits that ICT can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks." However, schools must, through their digital citizenship policy and practice, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. Further, all community members should embrace digital citizenship as a means of ethical and healthy use of technology.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school digital citizenship policy should help to ensure safe and appropriate use.

The development and implementation of such a strategy should involve all the stakeholders in a child's education from district and school administrators to faculty, staff, parents, members of the community and the students / pupils themselves.

The 360 Self Assessment is intended to help schools review their current digital citizenship policy and practice and provide:

- Management information and stimulus that can influence the production or review of e-safety policies and develop good practice.
- A process for identifying strengths and weaknesses.
- Opportunities for commitment and involvement from the whole school.
- A continuum for schools to discuss how they might move from a basic level provision for digital citizenship to practice that is aspirational and innovative.
- Accreditation for achieving highest level of digital citizenship through Generation Safe™ Gold and Platinum Medals.

The 360 Self Assessment is now available as an online tool, providing a more interactive and comprehensive method to review digital citizenship in schools.

Further details of the online tool and accreditation through Generation Safe™ Medals can be found at:
www.generationsafe360.org

How to use Generation Safe™ 360 Self Assessment

The self review tool enables you to review your school's current practice over four main topics:

A. POLICY & LEADERSHIP | B. EDUCATION | C. TECHNICAL INFRASTRUCTURE | D. E-SAFETY ACCOUNTABILITY

LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
There is little or nothing in place.	Policy and practice is being developed	Basic policy and practice is in place	Policy and practice is coherent and embedded	Policy and practice is aspirational and innovative

For each aspect, Gold Medal benchmark levels are shown with yellow outline

A record sheet is attached for schools to identify the level that matches their current practice for each aspect. By reading the descriptors for levels above the school's current level, it will be possible to identify the steps that are needed to progress further.

The record sheet also includes sections for comments – which schools may wish to use to clarify their choice of level or as an memory aid to further actions.

The sources of evidence column may help schools to share knowledge and information among those involved in the review. It may also be helpful to any external consultant or adviser that the school might wish to involve in its audit, review or policy development.

It is suggested that schools should use a whole school approach to the 360 Self Assessment. While it is helpful to identify a person or team to coordinate the review, it is essential that a wide range of members of the school community should be engaged in the process to ensure understanding and ownership. Once the school's current position has been established, the findings can then be used to draw up an action plan for development.

Links to resources

- The Internet Keep Safe Coalition (iKeepSafe): www.ikeepsafe.org
- Generation Safe™ online tools: www.ikeepsafe.org/gensafe
- South West Grid for Learning (SWGfL): www.swgfl.org.uk

Acknowledgements

iKeepSafe would like to acknowledge the SWGfL E-Safety Group who have been responsible for the vision and production of the Generation Safe™ 360 Self Assessment.

Copyright of this Self Review Tool is held by iKeepSafe.org and SWGfL. All rights reserved. This document may only be copied by authorized Generation Safe™ subscribers for educational, classroom and individual use only.

Send inquiries to legal@ikeepsafe.org.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication. However, neither iKeepSafe nor SWGfL can not guarantee its accuracy, nor can it accept liability in respect of the use of the material.

Topic 1 of 4

This division reflects the importance of having a clear vision and strategy for digital citizenship, with effective policies and leadership. This should be owned and understood by all stakeholders. There should be effective self-evaluation, accountability, reporting systems and sanctions.

Policy & Leadership > Responsibilities

This section allows schools to review the role of individuals and groups and to ensure that they have clearly understood responsibilities for digital citizenship and e-safety and that these responsibilities are being carried out. Are all stakeholders effectively engaged? Have policies become active documents that become part of the school culture?

Topic 1: Policy and Leadership

Section 1: Responsibilities

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Aspect 1 Administrators	There is no school administrator involvement in e-safety.	The school administrators are aware that an e-safety policy is being developed, but they are not involved in its development.	School administrators are involved in the development and approval of the e-safety policy.	School administrators are involved in the development and approval of the e-safety policy. There is an appointed e-safety administrator who is a member of the e-safety committee. School administrators are aware of their responsibilities with regard to digital citizenship. There are allocated resources to provide digital citizenship education.	School administrators are involved in the development and approval of the e-safety policy. There is a nominated e-safety administrator. All school administrators are aware of their responsibilities with regard to digital citizenship. School administrators receive regular monitoring reports on the implementation of the e-safety policy and on reported incidents. School administrators are involved in the promotion of digital citizenship in the wider community.
Aspect 2 E-Safety Commitee	There is no e-safety committee.	The school is in the process of establishing an e-safety committee.	The school has an e-safety committee with faculty/staff, parent, and student representation and a mission statement.	The school has an active e-safety committee with wide representation. It has clear lines of responsibility and accountability.	The school has an active e-safety committee with wide representation from within the school and the wider community. It has clear lines of responsibility and accountability which are understood by all members of the school. The committee is actively integrated and collaborating with other relevant groups in school.
Aspect 3 E-Safety Responsibilities	No one has responsibility for digital citizenship across the school	One or more members of faculty/staff have responsibility for digital citizenship, but there is little coordination of their work.	The school has a designated e-safety coordinator/officer with clear responsibilities, aligned with district (regional) and state guidelines.	The school has a designated e-safety coordinator/officer with clear responsibilities, aligned with district (regional) and state guidelines. These include leadership of the e-safety committee, faculty/staff training and awareness. A small group, including the principal, is responsible for monitoring incidents and handling sensitive issues (including Child Protection Services (CPS) or law enforcement as needed). Many staff take responsibility for digital citizenship.	The school has a designated e-safety coordinator/officer with clear responsibilities, aligned with district (regional) and state guidelines. These include leadership of the e-safety committee, faculty/staff training and awareness, commitment to and coordination of a digital citizenship program with the wider community. A small group, including the principal, is responsible for monitoring incidents and handling sensitive issues. All staff take active responsibility for digital citizenship.

What Evidence could you use?

- Minutes of administration meeting/ sub-committee meetings.
- Reports to school administration-- including monitoring reports.
- Minutes reports of e-safety committee.
- E-safety committee and administration bylaws.
- Administration training records / accreditation.
- E-safety committee minutes.
- E-safety committee bylaws.
- Other minutes and reports as relevant, including administration.
- Digital citizenship community programs.
- Job descriptions.
- Incident report logs and associated statistics.

Moving forward – the school might wish to consider: How do you engage all stakeholders (including faculty/staff, young people, parents and guardians, administrators and members of the community) in the establishment of the e-safety policy and their involvement in the e-safety committee and other relevant groups? Do all stakeholders know, understand and accept their responsibilities?

Topic 1 of 4

This division reflects the importance of having a clear vision and strategy for digital citizenship, with effective policies and leadership. This should be owned and understood by all stakeholders. There should be effective self-evaluation, accountability, reporting systems and sanctions.

Policy & Leadership > Policy Development

This section allows schools to review whether they have in place effective structures for making and reviewing e-safety policies, that digital citizenship is embedded in other relevant policies and that policy making is supported by effective reporting systems and sanctions. How effective are self-evaluation processes? Is digital citizenship regarded as a whole school issue? Is digital citizenship regarded as a child health and well-being issue rather than simply a technical issue? Do users know how, and to whom, to report incidents? Are they confident they will be taken seriously? Are sanctions enforced and are they clearly known, understood and respected?

Topic 1 — Policy and Leadership

Section 2 — Policy Development

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Aspect 1 Policy Development	There is no e-safety policy.	The school is in the process of establishing an e-safety policy.	The school has an e-safety policy, which is aligned with district (regional) and state standards.	The school has an e-safety policy, which is aligned with district (regional) and state guidelines and has been developed in consultation with a wide range of faculty/staff and students. There is "whole school ownership" of the policy. The policy is reviewed annually.	The school has an e-safety policy which is aligned with district (regional) and state guidelines and has been developed in consultation with the faculty/staff, students, parents and the wider community. There is widespread ownership of the policy. The policy is reviewed annually and more frequently in light of changes in technology or cyber incidents. The policy is an integral part of school improvement planning (eg CSIP).
Aspect 2 Policy Scope	There is no e-safety policy.	The school is in the process of establishing an e-safety policy.	The e-safety policy is limited to the use of the ICT systems, equipment and software in school.	The e-safety policy covers the use of the ICT systems, equipment and software, both on and off-campus. It also covers personal ICT equipment in school. It is comprehensive, including sections such as cyberbullying, data protection, passwords, filtering, digital and video images and use of mobile/handheld devices.	The e-safety policy covers the use of the ICT systems, equipment and software, both on and off-campus. It also covers personal ICT equipment in school. It is comprehensive, including sections such as cyberbullying, data protection, passwords, filtering, digital and video images and use of mobile/handheld devices. The policy clearly states the school's responsibility and commitment to take action over school-related cyber incidents that take place off-campus, and these policies are written into the RUP agreements. The e-safety policy is differentiated and age-related.
Aspect 3 Acceptable Use Policies	There are no acceptable use policies (AUPs).	AUPs are being developed.	AUPs are in place for students and faculty/staff.	AUPs are in place, signed by students, adult volunteers, community users, and faculty/staff. Clear policies ensure that young people and adults who are new to the school are informed of and required to sign RUPs. The title "Acceptable Use Policy" (AUP) has been changed to "Responsible Use Policy" (RUP) to emphasize students' active accountability in the safe and ethical use of technology.	RUPs include provisions developed by the e-safety committee. RUPs, which are differentiated by age and maturity, are in place for, and signed annually by faculty/staff, students, adult volunteers, and community users. The title "Acceptable Use Policy" has been changed to "Responsible Use Policy" to emphasize students' active accountability in the safe and ethical use of technology.

What Evidence could you use?

E-safety policy. Minutes of e-safety committee, administrators meeting/ sub-committees and other relevant groups. Review documents. Incident logs. School improvement plan (eg CSIP).

E-safety policy. Minutes of e-safety committee, administration meeting/ sub-committees and other relevant groups. Information for parents (eg letters, RUPs, newsletter, website). Information for students.

Responsible use policies (RUPs). Registration and volunteering policies and procedures.

Moving forward – the school might wish to consider: How do you engage all stakeholders (including faculty/staff, young people, parents and guardians, administrators and members of the community) in the establishment and review of the e-safety policy? How can the school ensure that all users clearly know and understand what is acceptable and responsible use and to understand why this is? Policies are active documents that become part of the school culture.

Topic 1 of 4

This division reflects the importance of having a clear vision and strategy for digital citizenship, with effective policies and leadership. This should be owned and understood by all stakeholders. There should be effective self-evaluation, accountability, reporting systems and sanctions.

Policy & Leadership > Policy Development

This section allows schools to review whether they have in place effective structures for making and reviewing e-safety policies, that digital citizenship is embedded in other relevant policies and that policy making is supported by effective reporting systems and sanctions. How effective are self-evaluation processes? Is digital citizenship regarded as a whole school issue? Is digital citizenship regarded as a child health and well-being issue rather than simply a technical issue? Do users know how, and to whom, to report incidents? Are they confident they will be taken seriously? Are sanctions enforced and are they clearly known, understood and respected?

Topic 1	Policy and Leadership					What Evidence could you use?
Section 2	Policy Development					
	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	Teams and department self-evaluation. Surveys. Whole school policies (eg behavior, anti bullying, student well-being, child abuse/ protection, and ICT).
Aspect 4 Self-Evaluation	Digital citizenship is not considered within the school's wider self-evaluation processes.	The school has begun to consider digital citizenship within the school's wider self-evaluation processes.	The school's wider self-evaluation processes address digital citizenship. There is reference to digital citizenship or e-safety in whole school documents. The school has identified and acknowledged some areas of strength and weakness and priorities for action.	Digital citizenship is a strong feature within the school's wider self-evaluation processes. The self-evaluation clearly acknowledges areas of strength and weakness and priorities for action. The school has made use of student and parent surveys to identify strengths, weaknesses and priorities in preparation for applying for the Generation Safe Gold Medal.	Digital citizenship is a strong feature within the school's wider self-evaluation processes. The self-evaluation acknowledges areas of strength and weakness and priorities for action. The school has made use of student and parent surveys to identifying strengths, weaknesses and priorities. The school has achieved or is in the process of achieving the Generation Safe Gold Medal. The school openly celebrates its digital citizenship successes in its wider self-evaluation processes.	
Aspect 5 Whole School	Digital citizenship or e-safety is not referred to in other whole school policies.	The school is beginning to link digital citizenship or e-safety into other whole school policies.	Digital citizenship or e-safety is referred to in other whole school policies eg behavior, anti-bullying, student well-being, child abuse/protection, and ICT policies.	There are clear and consistent links between the school e-safety policy and sections of other policies where there is reference to digital citizenship or e-safety (eg behavior, anti-bullying, student well-being, child abuse/protection, and ICT policies).	Digital citizenship is embedded in all relevant whole school policies. The school has carefully considered its approach to digital citizenship and provides a consistent digital citizenship message to all members of the school community, through a variety of media and activities that promote whole school input. This is particularly apparent in the references to digital citizenship or e-safety within such policies as behavior, anti-bullying, student well-being, child abuse/protection, and ICT policies.	

Moving forward – the school might wish to consider: How effective are the school self-evaluation processes and procedures? To what extent is e-safety regarded as a whole school issue, rather than just the responsibility of one section of the school (eg the ICT department)? To what extent is digital citizenship regarded as a child welfare issue rather than solely a technical issue?

Topic 1 of 4

This division reflects the importance of having a clear vision and strategy for digital citizenship, with effective policies and leadership. This should be owned and understood by all stakeholders. There should be effective self-evaluation, accountability, reporting systems and sanctions.

Policy & Leadership > Policy Development

This section allows schools to review whether they have in place effective structures for making and reviewing e-safety policies, that digital citizenship is embedded in other relevant policies and that policy making is supported by effective reporting systems and sanctions. How effective are self-evaluation processes? Is digital citizenship regarded as a whole school issue? Is digital citizenship regarded as a child health and well-being issue rather than simply a technical issue? Do users know how, and to whom, to report incidents? Are they confident they will be taken seriously? Are sanctions enforced and are they clearly known, understood and respected?

Topic 1: Policy and Leadership

Section 2: Policy Development

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Aspect 6 Disciplinary Action	There are no sanctions for technology abuse or misuse.	There are sanctions for technology abuse or misuse, but these are not linked to an agreed policy/ RUP and are not consistently enforced.	Sanctions for technology abuse or misuse are clearly stated in the e-safety policy. Users are aware of these sanctions.	Sanctions for technology abuse or misuse are clearly stated in the e-safety policy . Users are aware of these sanctions and understand their importance and generally adhere to the e-safety policy. A positive rewards policy balances the sanctions policy. Users understand that sanctions can be applied to off-campus incidents.	Sanctions for technology abuse or misuse are clearly stated in the e-safety policy. Users understand the importance of the sanctions and most users adhere to the e-safety policy. Positive rewards balance the sanctions within the policy. Users understand that sanctions can be applied to off-campus (eg cyberbullying). The school is consistent in reviewing and applying the e-safety policy, including a differentiated and appropriate range of sanctions.
Aspect 7 Reporting	Users are unclear about their responsibility to report cyber incidents and there is no clear process for reporting abuse.	Systems (including supervision where appropriate), and processes are in place for users to report cyber incidents and abuse (these are not yet consistently understood or consistently used). An E-Safety Contact List has been created.	Users understand their responsibility to report cyber incidents. They know and understand that there is a clear system for reporting abuse and understand that the processes must be followed consistently. Reports are logged for future assessing/ reviewing.	Users understand their responsibility to report cyber incidents. They use a clear system for reporting abuse and understand that processes must be followed consistently. Reports are logged and regularly assessed and reviewed. Users are confident that they can approach responsible persons if they have worries about actual, potential, or perceived cyber incidents. The school seeks support from local law enforcement when needed.	There are clearly known and understood systems for reporting cyber incidents. The culture of the school encourages all members of the school and its wider community to be vigilant in reporting issues using the schools protocols. Reports are logged and regularly assessed and reviewed. The school seeks support from local law enforcement when needed in dealing with e-safety issues. There are good links with outside agencies (eg law enforcement) who can help the school and members of the community in dealing with these issues. The school contributes to consistent reviewing/reporting practices.

What Evidence could you use?

Behavior and anti-bullying policies. Rewards and sanctions policies. On screen messages. RUPs.

Posters in classrooms. On screen messages. RUPs. Incident logs with evidence of reviewing and assessing. Communications with external agencies.

Moving forward – the school might wish to consider: Do users (young people and faculty/staff) know how and to whom they should report e-safety incidents? Are they confident that cyber incidents will be dealt with sympathetically and rigorously? Are there clear and proportionate sanctions for e-safety misuse? Are these clearly known, understood and respected?

Topic 1 of 4

This division reflects the importance of having a clear vision and strategy for digital citizenship, with effective policies and leadership. This should be owned and understood by all stakeholders. There should be effective self-evaluation, accountability, reporting systems and sanctions.

Policy & Leadership > **Communication Technologies**

This section allows schools to consider whether the digital citizenship topics related to the use of a wide range of "new technologies" has been sufficiently considered in wider policies and practice. Has the school maximized the educational potential of these technologies and considered how their safe use might be encouraged? Has the school encouraged professional discussion and understanding about the use of these technologies?

Topic 1	Policy and Leadership					
Section 3	Communication Technologies					
	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	What Evidence could you use?
Aspect 1 Mobile Phones and Personal Handheld Devices	There is no policy relating to the use of mobile phones and personal handheld devices.	A policy relating to the use of mobile phones and personal handheld devices is being developed.	The school has a policy relating to the use of mobile phones and personal handheld devices.	The school has implemented policies relating to the use of mobile phones and personal handheld devices. Users understand the risks associated with the use of these devices and are encouraged to be responsible users, both inside school (if allowed) and outside school. The school realizes the educational potential of these devices and is investigating how they might be used safely in school.	The school has implemented policies relating to the use of mobile phones/handheld devices. Users have a mature approach to their safe use. The school has realized the educational potential of these devices and has allowed/encouraged their safe use within school, where this is relevant to learning. There are clear and enforced sanctions for misuse. The school has consulted with parents and the wider community and gained their support for this policy.	RUPs. Policy for the use of mobile phones/handheld devices. Lesson plans. Consultation with parents/surveys.

Moving forward – the school might wish to consider: How is the school ensuring the safe use of these technologies, both on campus (where allowed) and off campus where there may be serious issues about use that is not monitored or filtered? Has the school realized the educational potential of these technologies and considered how their safe use might be encouraged, where relevant?

Topic 1 of 4

This division reflects the importance of having a clear vision and strategy for digital citizenship, with effective policies and leadership. This should be owned and understood by all stakeholders. There should be effective self-evaluation, accountability, reporting systems and sanctions.

Policy & Leadership > Communication Technologies

This section allows schools to consider whether the digital citizenship topics related to the use of a wide range of "new technologies" has been sufficiently considered in wider policies and practice. Has the school maximized the educational potential of these technologies and considered how their safe use might be encouraged? Has the school encouraged professional discussion and understanding about the use of these technologies?

Topic 1	Policy and Leadership
Section 3	Communication Technologies

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Aspect 2 Email, Chat, Social Networking, Instant Messaging, Blogging and Video Conferencing	There is no policy relating to the use of communication technologies such as email, chat, social networking, instant messaging, blogging, and video conferencing.	A policy relating to the use of communication technologies such as email, chat, social networking, instant messaging, blogging, and video conferencing is being developed.	The school has a policy relating to the use of communication technologies such as email, chat, social networking, instant messaging, and video conferencing. Users understand that their use of these systems will be monitored.	The school has implemented policies relating to the use, by faculty/staff and students, of communication technologies such as email, chat, social networking, instant messaging, and video conferencing. Users understand that their use of these systems will be monitored. They understand the risks associated with the use of these devices and are encouraged to be responsible users, both inside school (if allowed) and outside school. The school realizes the educational potential of new communication technology (eg social networking)and is investigating how they might be used safely in school.	The school has implemented policies relating to the use of communication technologies, by faculty/staff and students, such as email, chat, social networking, instant messaging, and video conferencing. Users understand that their use of these systems will be regularly monitored, with findings reported to the e-safety committee. They understand the risks associated with the use of these systems. The school has realized the educational potential of new communication technology and has allowed their safe use within school, where relevant to learning. There are clear and enforced sanctions for misuse. The school has consulted with parents and the wider community and gained their support for this policy.
Aspect 3 Digital and Video Images	There is no policy relating to the use and publication of digital and video images.	A policy relating to the use and publication of digital and video images is being developed.	The school has policies relating to the use and publication of digital and video images.	The school has understood and implemented policies relating to the use and publication of digital and video images. Parental permission forms are included in the RUPs for publication of images on the website and other publications. Similar permission is gained from older secondary age students, reflecting their personal rights. All members of the school, including faculty and staff, are educated about the risks associated with the taking, publication and distribution of images (and in particular the risks attached to publishing their own images on the internet).	The school has understood and implemented policies relating to the use and publication of digital and video images. Parental permission forms are included in the RUPs for publication of images on the website and other publications. Similar permission is gained from older secondary age students, reflecting their personal rights. Members of the school are encouraged to use digital and video images to promote the quality of their learning and understand the risks associated with the taking, publication and distribution of images (and in particular the risks attached to publishing their own images on the internet). Faculty/staff are encouraged to use digital and video images to record learning and to celebrate success, while being cautious about the nature of the activities being recorded and avoiding the potential for young people to be identified from published images.
Aspect 4 Website, Online Education, External Communications	There is no reference to digital citizenship or e-safety on the school's website, learning platform, newsletters, etc.	There are limited references to digital citizenship or e-safety on the school's website, learning platform, newsletters, etc.	The school's external communications (eg website, learning platform, newsletters, etc.) are used to provide information about digital citizenship or e-safety. The school has considered and addressed digital citizenship through these media.	The school encourages the use of external communications (eg website, learning platform, newsletters, etc.) and these are used to provide information about digital citizenship and celebrate the school's successes. The school ensures that good practice has been observed in the use of these media (eg use of digital and video images, copyright, identification of young people, publication of school calendars and protecting personal information) – ensuring that there is no risk to members of the school community through such publications.	The school encourages the use of external communications (eg website, learning platform, newsletters, etc.) that are used to provide information about digital citizenship, celebrate the school's successes and address (and capture) issues relevant to the digital citizenship of members of the wider community. The school ensures that good practice has been observed in the use of these media (eg use of digital and video images, copyright, identification of young people, publication of school calendars and protecting personal information) – ensuring that there is no risk to members of the school community through such publications. These policies and practices are regularly reviewed and reinforced. Care is taken to assess e-safety in the use of new communication technologies.

What Evidence could you use?

RUPs. Policies for the use of communications technologies. Lesson plans. Consultation with parents/surveys.

Policy for the use of digital and video images. RUPs (signed). Newsletters, website, VLE/learning platform. Lesson plans.

Newsletters, website, VLE/learning platform. Lesson plans.

Moving forward – the school might wish to consider: How is the school ensuring safe use of these technologies, both on campus (where allowed) and off campus? Has the school realized the educational potential of these technologies and considered how their safe use might be encouraged, where relevant?

Topic 1 of 4

This division reflects the importance of having a clear vision and strategy for digital citizenship, with effective policies and leadership. This should be owned and understood by all stakeholders. There should be effective self-evaluation, accountability, reporting systems and sanctions.

Policy & Leadership > **Communication Technologies**

This section allows schools to consider whether the digital citizenship topics related to the use of a wide range of "new technologies" has been sufficiently considered in wider policies and practice. Has the school maximized the educational potential of these technologies and considered how their safe use might be encouraged? Has the school encouraged professional discussion and understanding about the use of these technologies?

Topic 1	Policy and Leadership					What Evidence could you use?
Section 3	Communication Technologies					Policy documents. Faculty/staff handbooks.
	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	
Aspect 5 Professional Use Standards	The school has no policies or protocols in place for the use of new technologies for communications between the faculty, staff, and other members of the school and wider community.	The school is developing policies and protocols for the use of new technologies for communications between the faculty, staff, and other members of the school and wider community.	In consultation with the faculty and staff, the school has in place policies and protocols for the use of new technologies for communications between the faculty, staff and other members of the school and wider community. Faculty and staff follow the professional standards for teachers. Users know that monitoring systems are in place.	In consultation with the staff, the school has in place policies and protocols for the use of new technologies for communications between the faculty, staff and other members of the school and wider community. Faculty/staff follow professional standards for teachers. Faculty/staff understand the need for communication with students, parents, and members of the community to take place only through official school systems (eg school email, VLE, etc.) and that the communications must be professional in nature.	In consultation with the faculty and staff, the school has in place policies and protocols for the use of new technologies for communications between the faculty/staff and other members of the school and wider community. Faculty/ staff follow professional standards for teachers. Members of faculty/staff only use official school systems (eg school email, VLE, etc.) for communication with students, parents and members of the community. Reviews show that the culture of the school is reflected in the highly professional nature and content of these communications. The school encourages the use of new communication technologies but ensures that digital citizenship issues have been carefully considered and policies updated before they are adopted for use.	

Moving forward – the school might wish to consider: Has the school realized the educational potential of the new technologies and encouraged their use, where relevant, while ensuring that faculty/staff are protected from potential allegations relating to professional standards?

Topic 2 of 4

This topic reflects the importance of effective education and training for all stakeholders, in order to ensure that users know and understand the need for safe and secure use of ICT systems and handheld devices – both in school and in the wider community.

Education > Students

This section allows schools to review the extent to which they adequately prepare young people to become informed and responsible users - both within and outside school. Is digital citizenship fully embedded in all aspects of the school curriculum and other school activities? Does the school acknowledge and make full use of the contribution that young people can make to digital citizenship in and out of school?

Topic 2	Education					
Section 1	Students					
	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	What Evidence could you use?
Aspect 1 Digital Citizenship for Students	There is no planned program of digital citizenship for students.	A planned program of digital citizenship for students is being developed.	A planned student digital citizenship program takes place in computer labs/student health class/ ICT/ or other subjects and is regularly revisited. Students are aware of issues and are empowered to stay safe. Appropriate e-safety resources are used. The school is aware of the need to educate and protect vulnerable at-risk youth.	A planned student digital citizenship program takes place in computer labs/ student health class/ ICT/ or other subjects and is regularly revisited. The digital citizenship curriculum has breadth and progression, taking into account developments and innovations in new technologies. Students are aware of digital citizenship issues and understand and follow the e-safety and responsible use policies. Appropriate digital citizenship resources are used. The school is effective in the education and protection of at-risk youth. The school regularly evaluates the effectiveness and impact of digital citizenship programs.	A planned student digital citizenship program takes place and is fully embedded in all aspects of the curriculum in all grades and in other school activities, including before and after school programs. The digital citizenship program has breadth and progression, taking into account developments and innovations in new technologies. The program is regularly reviewed and revised. Students are aware of digital citizenship issues, and they understand and follow the e-safety and responsible use policies (RUPs). Digital citizenship resources are varied and appropriate. Digital citizenship messages are delivered using new technologies, in an engaged and relevant manner. Students are highly involved in digital citizenship education (eg through peer mentoring). The school is effective in the education and protection of youth who may be at risk because of their own and others' actions on-line. The school regularly evaluates the impact and effectiveness of digital citizenship programs.	Lesson plans. Classroom resources. Learning platform, VLE, website. Student journals and portfolios.
Aspect 2 Digital Literacy	There are no opportunities for students to gain an understanding of digital literacy skills.	Opportunities for students to gain an understanding of digital literacy skills are being developed.	Students are taught in some lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information. They have an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.	Students are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information. Faculty/staff and students use and understand "Creative Commons" licensing. There are many opportunities for them to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.	Students are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information. Faculty/staff and students use and understand "Creative Commons" licensing. There are many opportunities for them to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. The school actively provides systematic opportunities for students to develop the skills of safe and responsible online behavior. Faculty/staff and students acknowledge copyright and intellectual property rights in all their work.	Lesson plans. Classroom resources. Learning platform, VLE, website. Work samples and exercise books.

Moving forward – the school might wish to consider: Is digital citizenship education fully embedded in all aspects of the curriculum and other school activities, rather than just through ICT lessons? Does digital citizenship education help young people to become informed and responsible users – both in and out of school?

Topic 2 of 4

This topic reflects the importance of effective education and training for all stakeholders, in order to ensure that users know and understand the need for safe and secure use of ICT systems and handheld devices – both in school and in the wider community.

Education > Students

This section allows schools to review the extent to which they adequately prepare young people to become informed and responsible users - both within and outside school. Is digital citizenship fully embedded in all aspects of the school curriculum and other school activities? Does the school acknowledge and make full use of the contribution that young people can make to digital citizenship in and out of school?

Topic 2	Education					What Evidence could you use?
Section 1	Students					
	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	
Aspect 3 Student Contribution	The school does not acknowledge or use the high level of skills and knowledge of young people in the use of new technologies in its digital citizenship programs.	The school is developing opportunities to acknowledge and use the high level of skills and knowledge of young people in the use of new technologies in its digital citizenship programs.	The school acknowledges, learns from and uses the high level of skills and knowledge of young people in the use of new technologies. These contribute to the development of digital citizenship programs.	The school acknowledges, learns from and uses the high level of skills and knowledge of young people in the use of new technologies. The school involves students in digital citizenship campaigns and in peer mentoring, buddying and counseling programs within the school. Students are encouraged to provide feedback in reviews of e-safety related policies and responsible use policies (RUPs).	The school acknowledges, learns from and uses the high level of skills and knowledge of young people in the use of new technologies. Faculty/ staff frequently invite students to contribute through their knowledge and skills. The school involves students in digital citizenship campaigns and in peer mentoring, buddying and counseling programs and as student researchers. Students are encouraged to provide feedback in reviews of digital citizenship related policies and RUPs. Young people actively contribute to parent nights and family learning programs with digital citizenship as their focus.	Peer mentoring programs. Buddying programs. Contributions from children and young people in school publications/on school website/at parent nights.

Moving forward – the school might wish to consider: Does the school acknowledge and make full use of the contribution that young people can make to digital citizenship both in and out of school?

Topic 2 of 4

This topic reflects the importance of effective education and training for all stakeholders, in order to ensure that users know and understand the need for safe and secure use of ICT systems and handheld devices – both in school and in the wider community.

Education > Educators

This section allows schools to review the effectiveness of their e-safety training for school personnel. Do all school personnel receive adequate and on-going training and support in digital citizenship, enabling them to be safe and responsible users themselves? Are school personnel able to educate and support young people and others in e-safety and digital citizenship?

Topic 2	Education					
Section 2	Educators					
	LEVEL 1	**LEVEL 2**	**LEVEL 3**	**LEVEL 4**	**LEVEL 5**	
Aspect 1 Training for Administrators	There is no formal digital citizenship or e-safety training for administrators. Child abuse/protection training does not cover e-safety.	A formal digital citizenship training program is being developed for administrators. Child abuse/protection training will cover e-safety.	A planned program of formal digital citizenship training is made available to administrators. E-safety training is an integral part of child abuse/protection training and vice versa. An audit of digital citizenship/e-safety training needs is carried out. Digital citizenship training is included in the induction program for a new administrator. A digital citizenship professional development session has been held.	A planned program of formal digital citizenship training is made available to all administrators. E-safety training is an integral part of child abuse/protection training and vice versa. A review of training needs is carried out regularly and is addressed in performance management targets. All administrators have an up-to-date awareness of digital citizenship issues, current school e-safety policy and practices and child abuse/protection procedures. All new administrators receive training on digital citizenship issues as part of their induction program, ensuring that they fully understand the school e-safety and responsible use policies (RUPs).	A planned program of formal digital citizenship training is made available to all administrators. E-safety training is an integral part of child abuse/protection training and vice versa. An audit of training needs is carried out regularly and is addressed in performance management targets. All administrators understand current e-safety policy and practices and child abuse/protection procedures. All new administrators receive digital citizenship training as part of their induction program, ensuring that they fully understand the school e-safety policy and RUPs. The culture of the school ensures that school personnel support each other in sharing knowledge and good practice about digital citizenship issues. The school researches good practices in other schools. A range of administrators have taken accredited digital citizenship or e-safety courses.	
Aspect 2 Training for Faculty	There is no formal digital citizenship or e-safety training for faculty. Child abuse/protection training does not cover e-safety.	A formal digital citizenship training program for faculty is being developed. Child abuse/protection training will cover e-safety.	A planned program of formal digital citizenship training is made available to faculty. E-safety training is an integral part of child abuse/protection training and vice versa. An audit of digital citizenship/e-safety training needs is carried out. Digital citizenship training is included in the induction program for a new faculty member. A digital citizenship professional development session has been held.	A planned program of formal digital citizenship training is made available to all faculty. E-safety training is an integral part of child abuse/protection training and vice versa. A review of training needs is carried out regularly and is addressed in performance management targets. All faculty have an up-to-date awareness of digital citizenship issues, current school e-safety policy and practices and child abuse/protection procedures. All new faculty receive training on digital citizenship issues as part of their induction program, ensuring that they fully understand the school e-safety and responsible use policies (RUPs).	A planned program of formal digital citizenship training is made available to all faculty. E-safety training is an integral part of child abuse/protection training and vice versa. An audit of training needs is carried out regularly and is addressed in performance management targets. All faculty understand current e-safety policy and practices and child abuse/protection procedures. All new faculty receive digital citizenship training as part of their induction program, ensuring that they fully understand the school e-safety policy and RUPs . The culture of the school ensures that school personnel support each other in sharing knowledge and good practice about e-safety. The school researches good practices in other schools. A range of faculty have taken accredited digital citizenship or e-safety courses.	

What Evidence could you use?

Analysis of administrator training needs. Administrator training programs. Professional development portfolios. Induction programs. Good practice visits with other sites.

Analysis of faculty training needs. Faculty training programs. Professional development portfolios. Induction programs. Good practice visits with other sites.

Analysis of staff training needs. Staff training programs. Professional development portfolios. Induction programs. Good practice visits with other sites.

Moving forward – the school might wish to consider: Do all faculty/staff receive adequate induction and ongoing training and support in e-safety, to enable them to be safe and responsible users themselves and to be able educate and support young people and others in digital citizenship? Are all administrators aware, through training, of their responsibilities and of digital citizenship issues? Are administrators adequately prepared for their e-safety monitoring role?

Topic 2 of 4

This topic reflects the importance of effective education and training for all stakeholders, in order to ensure that users know and understand the need for safe and secure use of ICT systems and handheld devices – both in school and in the wider community.

Education > **Educators**

This section allows schools to review the effectiveness of their e-safety training for school personnel. Do all school personnel receive adequate and on-going training and support in digital citizenship, enabling them to be safe and responsible users themselves? Are school personnel able to educate and support young people and others in e-safety and digital citizenship?

Topic 2: Education

Section 2: Educators

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Aspect 3 Training for Staff	There is no formal digital citizenship or e-safety training for staff. Child abuse/ protection training does not cover e-safety.	A formal digital citizenship training program for staff is being developed. Child abuse/ protection training will cover e-safety.	A planned program of formal digital citizenship training is made available to staff. E-safety training is an integral part of child abuse/protection training and vice versa. An audit of digital citizenship/e-safety training needs is carried out. Digital citizenship training is included in the induction program for a new staff member. A digital citizenship professional development session has been held.	A planned program of formal digital citizenship training is made available to all staff. E-safety training is an integral part of child abuse/protection training and vice versa. A review of training needs is carried out regularly and is addressed in performance management targets. All staff have an up-to-date awareness of digital citizenship issues, current school e-safety policy and practices and child abuse/ protection procedures. All new staff receive training on digital citizenship issues as part of their induction program, ensuring that they fully understand the school e-safety and responsible use policies (RUPs).	A planned program of formal digital citizenship training is made available to all staff. E-safety training is an integral part of child abuse/protection training and vice versa. An audit of training needs is carried out regularly and is addressed in performance management targets. All staff understand current e-safety policy and practices and child abuse/protection procedures. All new staff receive digital citizenship training as part of their induction program, ensuring that they fully understand the school e-safety policy and RUPs. The culture of the school ensures that school personnel support each other in sharing knowledge and good practice about e-safety. The school researches good practices in other schools. A range of staff have taken accredited digital citizenship or e-safety courses.
Aspect 4 Training for School Counselor	There is no formal digital citizenship or e-safety training for school counselors. Child abuse/ protection training does not cover e-safety.	A formal digital citizenship training program for school counselors is being developed. Child abuse/ protection training will cover e-safety.	A planned program of formal digital citizenship training is made available to school counselors. E-safety training is an integral part of child abuse/ protection training and vice versa. An audit of digital citizenship/e-safety training needs is carried out. Digital citizenship training is included in the induction program for new school counselors. A digital citizenship professional development session has been held.	A planned program of formal digital citizenship training is made available to all school counselors. E-safety training is an integral part of child abuse/protection training and vice versa. A review of training needs is carried out regularly and is addressed in performance management targets. All school counselors have an up-to-date awareness of digital citizenship issues, current school e-safety policy and practices and child abuse/protection procedures. All new school counselors receive training on digital citizenship issues as part of their induction program, ensuring that they fully understand the school e-safety and responsible use policies (RUPs).	A planned program of formal digital citizenship training is made available to all school counselors. E-safety training is an integral part of child abuse/protection training and vice versa. An audit of training needs is carried out regularly and is addressed in performance management targets. All school counselors understand current e-safety policy and practices and child abuse/ protection procedures. All new school counselors receive digital citizenship training as part of their induction program, ensuring that they fully understand the school e-safety policy and RUPs. The culture of the school ensures that school personnel support each other in sharing knowledge and good practice about e-safety. The school researches good practices in other schools. A range of school counselors have taken accredited digital citizenship or e-safety courses.

What Evidence could you use?

Analysis of administrator training needs. Administrator training programs. Professional development portfolios. Induction programs. Good practice visits with other sites.

Analysis of faculty training needs. Faculty training programs. Professional development portfolios. Induction programs. Good practice visits with other sites.

Analysis of staff training needs. Staff training programs. Professional development portfolios. Induction programs. Good practice visits with other sites.

Moving forward – the school might wish to consider: Do all faculty/staff receive adequate induction and ongoing training and support in e-safety, to enable them to be safe and responsible users themselves and to be able educate and support young people and others in digital citizenship? Are all administrators aware, through training, of their responsibilities and of digital citizenship issues? Are administrators adequately prepared for their e-safety monitoring role?

Topic 2 of 4

This topic reflects the importance of effective education and training for all stakeholders, in order to ensure that users know and understand the need for safe and secure use of ICT systems and handheld devices – both in school and in the wider community.

Education > **Educators**

This section allows schools to review the effectiveness of their e-safety training for school personnel. Do all school personnel receive adequate and on-going training and support in digital citizenship, enabling them to be safe and responsible users themselves? Are school personnel able to educate and support young people and others in e-safety and digital citizenship?

Topic 2	Education					
Section 2	Educators					
	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	What Evidence could you use?
Aspect 5 Training for Librarian/ Media Specialist/ Technology Specialist	There is no formal digital citizenship or e-safety training for librarians/ technology specialists. Child abuse/ protection training does not cover e-safety.	A formal digital citizenship training program for librarians/ technology specialists is being developed. Child abuse/ protection training will cover e-safety.	A planned program of formal digital citizenship training is made available to librarians/ technology specialists. E-safety training is an integral part of child abuse/protection training and vice versa. An audit of digital citizenship/e-safety training needs is carried out. Digital citizenship training is included in the induction program for librarians/technology specialists. A digital citizenship professional development session has been held.	A planned program of formal digital citizenship training is made available to all librarians/technology specialists. E-safety training is an integral part of child abuse/ protection training and vice versa. A review of training needs is carried out regularly and is addressed in performance management targets. All librarians/technology specialists have an up-to-date awareness of digital citizenship issues, current school e-safety policy and practices and child abuse/ protection procedures. All new librarians/ technology specialists receive training on digital citizenship issues as part of their induction program, ensuring that they fully understand the school e-safety and responsible use policies (RUPs).	A planned program of formal digital citizenship training is made available to all librarians/technology specialists. E-safety training is an integral part of child abuse/protection training and vice versa. An audit of training needs is carried out regularly and is addressed in performance management targets. All librarians/ technology specialists understand current e-safety policy and practices and child abuse/protection procedures. All new librarian/technology specialists receive digital citizenship training as part of their induction program, ensuring that they fully understand the school e-safety policy and RUPs. The culture of the school ensures that school personnel support each other in sharing knowledge and good practice about e-safety. The school researches good practices in other schools. A range of librarian/technology specialists have taken accredited digital citizenship or e-safety courses.	Analysis of school counselor training needs. School counselor training programs. Professional development portfolios. Induction programs. Good practice visits with other sites. Analysis of librarian/ technology specialist training needs. Librarian/technology specialist training programs. Professional development portfolios. Induction programs. Good practice visits with other sites.
Aspect 6 Training for Network Administrator	There is no formal digital citizenship or e-safety training for network administrators. Child abuse/ protection training does not cover e-safety.	A formal digital citizenship training program for network administrators is being developed. Child abuse/ protection training will cover e-safety.	A planned program of formal digital citizenship training is made available to network administrators. E-safety training is an integral part of child abuse/protection training and vice versa. An audit of digital citizenship/e-safety training needs is carried out. Digital citizenship training is included in the induction program for a new network administrator. A digital citizenship professional development session has been held.	A planned program of formal digital citizenship training is made available to all network administrators. E-safety training is an integral part of child abuse/protection training and vice versa. A review of training needs is carried out regularly and is addressed in performance management targets. All network administrators have an up-to-date awareness of digital citizenship issues, current school e-safety policy and practices and child abuse/protection procedures. All new network administrators receive training on digital citizenship issues as part of their induction program, ensuring that they fully understand the school e-safety and responsible use policies (RUPs).	A planned program of formal digital citizenship training is made available to all network administrators. E-safety training is an integral part of child abuse/protection training and vice versa. An audit of training needs is carried out regularly and is addressed in performance management targets. All network administrators understand current e-safety policy and practices and child abuse/protection procedures. All new network administrators receive digital citizenship training as part of their induction program, ensuring that they fully understand the school e-safety policy and RUPs. The culture of the school ensures that school personnel support each other in sharing knowledge and good practice about e-safety. The school researches good practices in other schools. A range of network administrators have taken accredited digital citizenship or e-safety courses.	Analysis of network administrator training needs. Network administrator training programs. Professional development portfolios. Induction programs. Good practice visits with other sites.

Moving forward – the school might wish to consider: Do all faculty/staff receive adequate induction and ongoing training and support in e-safety, to enable them to be safe and responsible users themselves and to be able educate and support young people and others in digital citizenship? Are all administrators aware, through training, of their responsibilities and of digital citizenship issues? Are administrators adequately prepared for their e-safety monitoring role?

Topic 2 of 4

This topic reflects the importance of effective education and training for all stakeholders, in order to ensure that users know and understand the need for safe and secure use of ICT systems and handheld devices – both in school and in the wider community.

Education > Educators

This section allows schools to review the effectiveness of their e-safety training for school personnel. Do all school personnel receive adequate and on-going training and support in digital citizenship, enabling them to be safe and responsible users themselves? Are school personnel able to educate and support young people and others in e-safety and digital citizenship?

Topic 2	Education				
Section 2	Educators				
	LEVEL 1	**LEVEL 2**	**LEVEL 3**	**LEVEL 4**	**LEVEL 5**
Aspect 7 Training for School Nurse	There is no formal digital citizenship or e-safety training for school nurses. Child abuse/ protection training does not cover e-safety.	A formal digital citizenship training program for school nurses is being developed. Child abuse/ protection training will cover e-safety.	A planned program of formal digital citizenship training is made available to school nurses. E-safety training is an integral part of child abuse/protection training and vice versa. An audit of digital citizenship/e-safety training needs is carried out. Digital citizenship training is included in the induction program for a new school nurse. A digital citizenship professional development session has been held.	A planned program of formal digital citizenship training is made available to all school nurses. E-safety training is an integral part of child abuse/protection training and vice versa. A review of training needs is carried out regularly and is addressed in performance management targets. All school nurses have an up-to-date awareness of digital citizenship issues, current school e-safety policy and practices and child abuse/protection procedures. All new school nurses receive training on digital citizenship issues as part of their induction program, ensuring that they fully understand the school e-safety and responsible use policies (RUPs).	A planned program of formal digital citizenship training is made available to all school nurses. E-safety training is an integral part of child abuse/ protection training and vice versa. An audit of training needs is carried out regularly and is addressed in performance management targets. All school nurses understand current e-safety policy and practices and child abuse/protection procedures. All new school nurses receive digital citizenship training as part of their induction program, ensuring that they fully understand the school e-safety policy and RUPs. The culture of the school ensures that school personnel support each other in sharing knowledge and good practice about e-safety. The school researches good practices in other schools. A range of school nurses have taken accredited digital citizenship or e-safety courses.
Aspect 8 Training for Safe Schools Coordinator	There is no formal digital citizenship or e-safety training for safe schools coordinator. Child abuse/ protection training does not cover e-safety.	A formal digital citizenship training program for safe schools coordinators is being developed. Child abuse/ protection training will cover e-safety.	A planned program of formal digital citizenship training is made available to safe schools coordinator. E-safety training is an integral part of child abuse/protection training and vice versa. An audit of digital citizenship/e-safety training needs is carried out. Digital citizenship training is included in the induction program for a new safe schools coordinator. A digital citizenship professional development session has been held.	A planned program of formal digital citizenship training is made available to all safe schools coordinators. E-safety training is an integral part of child abuse/protection training and vice versa. A review of training needs is carried out regularly and is addressed in performance management targets. All safe schools coordinators have an up-to-date awareness of digital citizenship issues, current school e-safety policy and practices and child abuse/ protection procedures. All new safe schools coordinators receive training on digital citizenship issues as part of their induction program, ensuring that they fully understand the school e-safety and responsible use policies (RUPs).	A planned program of formal digital citizenship training is made available to all safe schools coordinators. E-safety training is an integral part of child abuse/protection training and vice versa. An audit of training needs is carried out regularly and is addressed in performance management targets. All safe schools coordinators understand current e-safety policy and practices and child abuse/protection procedures. All new safe schools coordinators receive digital citizenship training as part of their induction program, ensuring that they fully understand the school e-safety policy and RUPs. The culture of the school ensures that school personnel support each other in sharing knowledge and good practice about e-safety. The school researches good practices in other schools. A range of safe schools coordinators have taken accredited digital citizenship or e-safety courses.

What Evidence could you use?

Analysis of school nurse training needs. School nurse training programs. Professional development portfolios. Induction programs. Good practice visits with other sites.

Analysis of safe schools coordinator training needs. Safe schools coordinator training programs. Professional development portfolios. Induction programs. Good practice visits with other sites.

Moving forward – the school might wish to consider: Do all faculty/staff receive adequate induction and ongoing training and support in e-safety, to enable them to be safe and responsible users themselves and to be able educate and support young people and others in digital citizenship? Are all administrators aware, through training, of their responsibilities and of digital citizenship issues? Are administrators adequately prepared for their e-safety monitoring role?

Topic 2 of 4

This topic reflects the importance of effective education and training for all stakeholders, in order to ensure that users know and understand the need for safe and secure use of ICT systems and handheld devices – both in school and in the wider community.

Education > Parents and Guardians

This section allows schools to review the extent to which they involve parents and guardians in digital citizenship programs and the effectiveness of their involvement. Does the school acknowledge the importance of parents and guardians in digital citizenship and the monitoring of the children's online experiences (particularly off-campus)? Does it provide sufficient opportunities to provide information and support to parents and guardians to allow them to carry out this role?

Topic 2	Education
Section 3	Parents and Guardians

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	What Evidence could you use?
Aspect 1 Parental Education	The school does not provide opportunities for parents to receive education or information about digital citizenship.	The school is developing opportunities for parents to receive education or information about digital citizenship.	The school provides opportunities for parents and guardians to receive education or information about digital citizenship. Parents and guardians are aware of and endorse (by signature) the student RUP. All parents have received digital citizenship information.	The school provides opportunities for parents to receive regular education or information about digital citizenship. Parents and guardians are aware of and endorse (by signature) the student RUP. All parents have received digital citizenship information. The school understands the importance of the role of parents and guardians in digital citizenship education and in the monitoring of the children's on-line experiences (particularly off-campus). Parents and guardians know who to contact if they are worried about digital citizenship issues.	The school provides opportunities for parents and guardians to receive regular education or information about digital citizenship. Parents and guardians are aware of and endorse (by signature) the student RUP. All parents and guardians have received a copy of digital citizenship information. The school understands the importance of the role of parents and guardians in digital citizenship education and in the monitoring of children's on-line experiences (particularly off-campus). Parents and guardians know who to contact if they are worried about digital citizenship issues. The school takes every opportunity to help parents and guardians understand digital citizenship issues through parent nights, newsletters, website, VLE etc. Parents and guardians know about the school's reporting procedure and how to use it effectively. The school is effective in engaging "hard to reach" parents and guardians in digital citizenship programs.	RUPs. Letters to parents, newsletters, website, VLE. Parent nights/sessions. Family learning events.

Moving forward – the school might wish to consider: Does the school acknowledge the importance of parents and guardians in digital citizenship education and the monitoring / regulation of the children's online experiences (particularly off-campus)? Does it provide sufficient opportunities to provide information and support to parents and guardians to allow them to carry out this role? Does the school also provide this service to other members of the community, through its extended services?

Topic 2 of 4

This topic reflects the importance of effective education and training for all stakeholders, in order to ensure that users know and understand the need for safe and secure use of ICT systems and handheld devices – both in school and in the wider community.

Education > Community Outreach

This section allows schools to review the extent to which it involves the wider community in its digital citizenship programs. Does the school acknowledge the importance of the wider community in the campaign for positive digital citizenship? Does it provide sufficient opportunities to inform and support members of the wider community? Does the school take advantage of the diverse range of skills and experience available in the wider community?

Topic 2	Education					What Evidence could you use?
Section 4	Community Outreach					
	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	Letters to community members, newsletters, website, VLE. Family learning events.
Aspect 1 Community Understanding	The school does not provide opportunities for members of its wider community to gain information and understanding about digital citizenship.	The school is developing opportunities for members of its wider community to gain information and understanding about digital citizenship.	The school provides opportunities for members of its wider community to gain information and understanding about digital citizenship.	The school provides opportunities for members of its wider community to gain information and understanding about digital citizenship. Family learning courses are offered in ICT, media literacy and digital citizenship. Plans are being developed to increase community involvement.	The school provides opportunities for members of its wider community to gain information and understanding about digital citizenship. Family learning courses are offered in ICT, media literacy and digital citizenship. The school recognizes the significant role that the local community can play in improving the quality of education and levels of aspiration. The culture of the school ensures that members of the local community are involved, whenever possible, in the planning of community programs and in the delivery of programs in school.	

Moving forward – the school might wish to consider: Does the school acknowledge the importance of parents and guardians in digital citizenship education and the monitoring / regulation of the children's online experiences (particularly off-campus)? Does it provide sufficient opportunities to provide information and support to parents and guardians to allow them to carry out this role? Does the school also provide this service to other members of the community, through its extended services?

Topic 3 of 4

This topic reflects the importance of having effective systems in place to ensure the security of the school's ICT systems, system users and personal data. These should be owned and understood by all users and should be subject to regular review and updating, in the light of constantly changing technology and the development of new security threats.

Technical Infrastructure > Passwords

This section allows the school to reflect on whether its password policies are effective and whether they are clearly understood and implemented. Does the school continually review and update its practice in the light of new information?

Topic 3	Technical Infrastructure
Section 1	Passwords

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	What Evidence could you use?
Aspect 1 Password Security	There is no agreed password policy	Password policies are being developed	The school has a password policy which applies to all users. Passwords are secure and are consistent with district (regional), state, and federal guidelines (eg CIPA).	The school has clearly understood and accepted policies relating to the use of passwords. Passwords are secure and consistent with district (regional), state, and federal information security guidelines (eg CIPA). Password changes are regularly enforced. Users understand that passwords must never be shared. There are clear procedures for the provision of new passwords, with forced changes at first login. All users have clearly defined access rights to school ICT systems. There are clear policies for the use and control of the "master/administrator" passwords.	The school has clearly understood and accepted policies relating to the use of passwords. Passwords are secure and fully compliant with district (regional), state, and federal information security guidelines (eg CIPA), with rigorous testing against these standards. Password changes are regularly enforced. Users understand that passwords must never be shared. There are clear procedures for the provision of new passwords, with forced changes at first login. All users have clearly defined access rights to school ICT systems. There are clear policies for the use and control of the "master/administrator" passwords. There are regular audits of user logins to check for anonymous or unauthorized logins. There is regular testing of systems to ensure that the password security policy is being correctly implemented.	Password security policy. Logs and audits. RUPs. Faculty/staff handbooks.

Moving forward – the school might wish to consider: How does the school ensure that users understand and accept the importance of password security and follow the school's password security policy, using strong passwords that are changed regularly? Is the school aware of, and reviewing practice as a result of comprehensive current guidance from district (regional), state, and federal information security guidelines (eg CIPA)?

Topic 3 of 4

This topic reflects the importance of having effective systems in place to ensure the security of the school's ICT systems, system users and personal data. These should be owned and understood by all users and should be subject to regular review and updating, in the light of constantly changing technology and the development of new security threats.

Technical Infrastructure > Services

This section allows schools to review the security of their infrastrucure and whether it meets the best practice standards offered by industry leaders (eg ISPs), government regulations (eg COPPA) and local law enforcement. Are secure systems in place? Are they known, understood and rigorously enforced? Is there adequate separation of responsibilities? Is the school confident that policy and good practice ensure that all personal data is safe from risk of loss, misuse and unauthorized access?

Topic 3	Technical Infrastructure					What Evidence could you use?
Section 2	Services					
	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	Filtering policy. Monitoring logs and audits. Review documents (internal and external). RUPs. Monitoring logs and audits. Review documents (internal and external). RUPs.
Aspect 1 Filtering	A filtering system is not in place.	A filtering system is in place.	A filtering system with enhanced user levels is in place. Differential filtering is in place to encourage responsible use and apply sanctions for misuse.	A filtering system with enhanced user levels is in place. Differential filtering is in place to encourage responsible use and apply sanctions for misuse. The school has monitoring in place to complement the filtering. The school has a weekly monitoring process and takes action when breaches of the filtering policy are revealed. There is a clear route for reporting and managing changes to the filtering system.	A filtering system with enhanced user levels is in place. Differential filtering is in place to encourage responsible use and apply sanctions for misuse. The school has monitoring in place to complement the filtering. The school keeps and carries out daily monitoring of the filtering logs and takes action when breaches of the filtering policy are revealed. A clear policy is in place concerning requests for and records of changes to the filtering system, with adequate separation of responsibilities and regular oversight by senior leaders. Evidence from monitoring and filtering logs shows that users have a mature approach and that there are very few incidents of misuse. The school is therefore able to take an appropriate and balanced approach to filtering, in the knowledge that users have adopted safe online behavior.	
Aspect 2 Technical Security	The school does not meet the e-safety technical requirements outlined in district (regional), state, and federal guidelines (eg CIPA), and responsible use policies (RUPs).	The school meets the e-safety technical requirements outlined in district (regional), state, and federal guidelines (eg CIPA), and RUPs.	The school meets the e-safety technical requirements outlined in district (regional), state, and federal guidelines (eg CIPA), and RUPs. There are regular reviews and audits of the safety and security of the school ICT systems.	The school meets the e-safety technical requirements outlined in district (regional), state, and federal guidelines (eg CIPA), and RUPs. There are regular reviews and audits of the safety and security of school ICT systems, with oversight from senior leaders and these have an impact on policy and practice. The school's ICT infrastructure is secure and is not open to misuse or malicious attack.	The school meets the e-safety technical requirements outlined. School practice reflects up-to-date advancements in security, providing protection from new security threats as they arise, as outlined in district (regional), state, and federal guidelines (eg CIPA), and RUPs. There are regular reviews and audits of the safety and security of school ICT systems with oversight from senior leaders and these have an impact on policy and practice. Internal reviews are augmented by rigorous external reviews of the security of school systems. School practice reflects up-to-date advancements in security, providing protection from new security threats as they arise.	

Moving forward – the school might wish to consider: Is the school confident that the school ICT systems meet current e-safety technical requirements and users know and understand the importance of following these technical requirements? Is there an adequate separation of responsibilities among those with responsibility for managing the systems? Does the filtering provide security for users, while allowing the greatest benefit available from educational use of the internet? Is the filtering complemented by effective monitoring?

Topic 3 of 4

This topic reflects the importance of having effective systems in place to ensure the security of the school's ICT systems, system users and personal data. These should be owned and understood by all users and should be subject to regular review and updating, in the light of constantly changing technology and the development of new security threats.

Technical Infrastructure > Services

This section allows schools to review the security of their infrastrucure and whether it meets the best practice standards offered by industry leaders (eg ISPs), government regulations (eg COPPA) and local law enforcement. Are secure systems in place, are they known, understood and rigorously enforced? Is there adequate separation of responsibilities? Is the school confident that policy and good practice ensure that all personal data is safe from risk of loss, misuse and unauthorized access?

Topic 3	Technical Infrastructure					What Evidence could you use?
Section 2	Services					Personal Data Policy. Job descriptions.
	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	
Aspect 3 Personal Data	There is no agreed upon Personal Data Policy.	A Personal Data Policy is being developed.	The school has a Personal Data Policy which adheres to the Children's Online Privacy Protection Act (COPPA), and relevant district (regional), state, and federal guidelines (eg CIPA). All faculty/ staff know and understand the need to ensure the safekeeping of personal data, minimizing the risk of its loss or misuse.	The school has a Personal Data Policy which adheres to the Children's Online Privacy Protection Act (COPPA), and relevant district (regional), state, and federal guidelines (eg CIPA). All faculty/staff know and understand the need to ensure the safe keeping of personal data, minimizing the risk of its loss or misuse. Clear policies about the secure handling, transfer and disposal of data (passwords, encryption, and removable media) are known, understood and adhered to by users. Password protection is enhanced by the use of encryption and/or two factor authentication for the handling or transfer of sensitive data. The school has appointed a Senior Risk Information Officer/ Data Protection Officer and Information Asset Owners.	The school has a Personal Data Policy which adheres to the Children's Online Privacy Protection Act (COPPA), and relevant district (regional), state, and federal guidelines (eg CIPA). Faculty/ staff know and understand the need to ensure the safe keeping of personal data, minimizing the risk of its loss or misuse. Clear policies about the secure handling and transfer of data (passwords, encryption, and removable media) are known, understood and adhered to by users.. Password protection is enhanced by the use of encryption and/or two factor authentication for the handling or transfer of sensitive data. The school has appointed a Senior Risk Information Officer/Data Protection Officer and Information Asset Owners. There is a clear procedure in place for audit logs to be kept and for reporting, managing and recovering from information risk incidents	

Moving forward – the school might wish to consider: Is the school confident that policy and good practice ensure that all personal data is safe from risk of loss, misuse and unauthorized access? Are faculty/staff aware of their responsibilities? Is the school aware of, and reviewing practice as a result of, comprehensive current guidance from district (regional), state, and federal information security guidelines (eg CIPA)?

Topic 4 of 4

This topic reflects the importance of a school understanding of the effectiveness of its policies and practices and how they impact e-safety outcomes. Such an understanding will motivate school leaders to review incidents for emerging patterns and improve policies and practices to increase digital citizenship.

E-Safety Accountability > Protocol Assessment

This section allows schools to review and assess the effectiveness of its e-safety policy and practice. Have programs for reviewing, recording and reporting been built into the e-safety policy and practice? Does the school have ways in which it can measure the effectiveness of the e-safety policy and its programs? Is there a commitment to working with other schools and agencies to share evidence of impact and help ensure the development of consistent and effective local strategy on digital citizenship?

Topic 4 E-Safety Accountability

Section 1 Protocol Assessment

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Aspect 1 Evaluate and Assess Incidents	There is no policy for reviewing cyber incidents.	A policy for reviewing cyber incidents is being developed.	Cyber incidents are reviewed and records are kept. The records are reviewed and reported to the administration. Parents are informed of cyber incidents, as relevant.	Cyber incidents are recorded and reviewed. The records are reviewed and reported to the school administration, district (regional) administrators, law enforcement, and Child Protective Services (CPS). Reviewing and reporting of incidents contributes to policy development and the practice of digital citizenship within the school. Parents are specifically informed of cyber incidents involving their children. As part of the school's digital citizenship campaign, all parents are informed of patterns in cyber incidents.	Cyber incidents are recorded and reviewed. The records are reviewed and reported to the school administration, district (regional) administrators, law enforcement, and Child Protective Services (CPS). Reviewing and reporting of incidents contributes to policy development and the practice of digital citizenship within the school. Parents are specifically informed of cyber incidents involving their children. As part of the school's digital citizenship campaign, all parents are informed of patterns in cyber incidents. The school actively cooperates with other agencies to help ensure the development of a consistent and effective local digital citizenship strategy.
Aspect 2 Evaluate and Adjust Policy	There is no procedure for tracking the impact of the e-safety policy and practice.	Procedure for tracking the impact of the e-safety policy and practice is being developed.	The impact of the e-safety policy and practice is reviewed through the use of cyber incident logs, behavior/ bullying logs, and surveys of faculty/staff, students, parents.	The impact of the e-safety policy and practice is reviewed through the use of cyber incident logs, behavior/bullying logs, and surveys of faculty/staff, students, parents. The school reviews the effectiveness of e-safety support received from external agencies. There is balanced professional debate about the evidence taken from the data (ie the logs/surveys) and the impact of preventative work (eg digital citizenship programs).	The impact of the e-safety policy and practice is reviewed through the use of cyber incident logs, behavior/bullying logs, surveys of faculty/ staff, students, parents. The school reviews the effectiveness of e-safety support received from external agencies. There is balanced professional debate about the evidence taken from the data (ie the logs/surveys) and the impact of preventative work (eg digital citizenship education, awareness and training). The evidence of impact is shared with other schools and external agencies to help ensure the development of a consistent and effective local digital citizenship strategy.

What Evidence could you use?

Incident logs and audits/reviews. School improvement plan (eg CSIP). Minutes of meetings of relevant groups and committees, including administration. Monitoring reports.

Minutes of meetings of relevant groups and committees, including administration. Monitoring reports.

Moving forward – the school might wish to consider: Has provision for monitoring, recording and reporting been built into the e-safety policy and practice? Does the school have ways in which it can measure the effectiveness of the e-safety policy and provision? Is there a commitment to working with other schools and agencies to share evidence of impact and help ensure the development of a consistent and effective local digital citizenship strategy?

iKeepSafe Generation Safe 360 Self Assessment Tool

GENERATION SAFE™ 360 SELF ASSESSMENT: PRINTABLE VERSION

R1

Record Sheet 1

This record sheet should be used with the Generation Safe™ 360 Self Assessment. Schools should indicate in the Level columns which level best illustrates their current position for that aspect. Comments and evidence sources may be added as relevant.

Gold Medal benchmark levels are shown with yellow outline

Topic 1 — Policy and Leadership

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	COMMENT	SOURCE OF EVIDENCE
Section 1 — Responsibilities							
Aspect 1 Administrators							
Aspect 2 E-Safety Committee							
Aspect 3 E-Safety Responsibilities							
Section 2 — Policy Development							
Aspect 1 Policy Development							
Aspect 2 Policy Scope							
Aspect 3 Acceptable Use Policies							
Aspect 4 Self-Evaluation							
Aspect 5 Whole School							
Aspect 6 Disciplinary Action							
Aspect 7 Reporting							

Record Sheet 1

This record sheet should be used with the SWGfL E-Safety Self Review Tool. Schools should indicate in the Level columns which level best illustrates their current position for that aspect. Comments and evidence sources may be added as relevant.

Gold Medal benchmark levels are shown with yellow outline

Topic 1	Policy and Leadership						
	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	COMMENT	SOURCE OF EVIDENCE
Section 3	Communication Technologies						
Aspect 1 Mobile Phones and Personal Handheld Devices							
Aspect 2 Email, Chat, Social Networking, Instant Messaging, Blogging and Video Conferencing							
Aspect 3 Digital and Video Images							
Aspect 4 Website, Online Education, External Communications							
Aspect 5 Professional Use Standards							

Record Sheet 2

This record sheet should be used with the Generation Safe™ 360 Self Assessment. Schools should indicate in the Level columns which level best illustrates their current position for that aspect. Comments and evidence sources may be added as relevant.

Gold Medal benchmark levels are shown with yellow outline

Topic 2	Education							
	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	COMMENT	SOURCE OF EVIDENCE
Section 1	**Students**						
Aspect 1 Digital Citizenship for Students							
Aspect 2 Digital Literacy							
Aspect 3 Student Contribution							
Section 2	**Educators**						
Aspect 1 Training for Administrators							
Aspect 2 Training for Faculty							
Aspect 3 Training for Staff							
Aspect 4 Training for School Counselor							
Aspect 5 Training for Librarian/ Media Specialist/ Technology Specialist							
Aspect 6 Training for Network Administrator							
Aspect 7 Training for School Nurse							
Aspect 8 Training for Safe Schools Coordinator							

Record Sheet 2

This record sheet should be used with the Generation Safe™ 360 Self Assessment. Schools should indicate in the Level columns which level best illustrates their current position for that aspect. Comments and evidence sources may be added as relevant.

Gold Medal benchmark levels are shown with yellow outline

Topic 2	Education	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	COMMENT	SOURCE OF EVIDENCE
Section 3	Parents and Guardians							
Aspect 1 Parental Education					★			
Section 4	Community Outreach							
Aspect 1 Community Understanding				★				

Topic 3	Technical Infrastructure	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	COMMENT	SOURCE OF EVIDENCE
Section 1	Passwords							
Aspect 1 Password Security					★			
Section 2	Services							
Aspect 1 Filtering					★			
Aspect 2 Technical Security				★				
Aspect 3 Personal Data				★				

Record Sheet 3

This record sheet should be used with the Generation Safe™ 360 Self Assessment. Schools should indicate in the Level columns which level best illustrates their current position for that aspect. Comments and evidence sources may be added as relevant.

Gold Medal benchmark levels are shown with yellow outline

Topic 4	E-Safety Accountability						
	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	COMMENT	SOURCE OF EVIDENCE
Section 1	Protocol Assessment						
Aspect 1 Evaluate and Assess Incidents							
Aspect 2 Evaluate and Adjust Policy							

Name of School	
Contact Person	
School Address	
Email Address	
Telephone Number	

© 2011 iKeepSafe.org and SWGfL. All rights reserved.
This document may only be copied by authorized Generation Safe™ subscribers for educational, classroom and individual use only. Send inquiries to legal@ikeepsafe.org.

Internet Keep Safe Coalition, 1401 K Street N.W., Suite 600, Washington, D.C. 20005,
Phone: 202-587-5583, Fax: 202-737-4097 (“Attention: iKeepSafe”), Toll Free: 1-866-794-7233,
E-mail: info@iKeepSafe.org, Website: www.ikeepsafe.org