The Scottish Government
Riaghaltas na h-Alba

360 degree safe

SCHOOL E-SAFETY
SELF REVIEW TOOL

The South West Grid for Learning, Belvedere House,
Woodwater Park, Pynes Hill, Exeter, Devon, UK, EX2 5WS.
Tel: 0845 601 3203 **Fax:** 01392 366 494
Email: esafety@swgfl.org.uk
Website: www.swgfl.org.uk

www.360safescotland.org.uk

Contents

Introduction

The development and expansion of the use of ICT / computing, and particularly of the internet, is transforming learning and teaching in schools. The Scottish Government has set out it vision for ICT in Education as follows:

"Scotland's educators, learners and parents take full advantage of the opportunities offered by technology in order to raise attainment, ambition and opportunities for all." www.scotland.gov.uk/Topics/Education/Schools/SSDN

There is a large body of evidence that recognises the benefits that the use of digital technologies 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, more recently through significant investment in one to one devices. It is important for schools, through their e-safety policy and practice, to 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

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 e-safety 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 the Headteacher / Principal and Governors / Directors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students / pupils themselves.

The Self Review Tool is intended to help schools to review their current e-safety 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 e-safety to practice that is aspirational and innovative.

This online self-review tool has been adapted to take account of legislation, structure and practice in Scotland. It is suitable for local authority schools and independent schools. Independent schools who want further specific support, for example on training of governors will find this in the version of the tool used in the rest of the UK at www.360safe.org.uk. Schools may wish to use this PDF version of the tool's content as an aid to carrying out their online review. However, it is strongly recommended that schools should not use this PDF version alone – the online tool provided a more interactive and comprehensive method to review their E-Safety.

How to use the Self Review Tool

The 360 degree safe self-review tool enables you to review your school's current practice over four main elements, based on the PIES model:

A. POLICY & LEADERSHIP

B. INFRASTRUCTURE

C. EDUCATION

D. STANDARDS

Each element includes a number of strands, which in turn include a number of aspects. Schools may choose to work through the tool in the order that is offered, or may alternatively take elements, strands or aspects individually to suit their own circumstances. Each aspect has statements at five levels of maturity which range as below:

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

For each aspect, the benchmark level for the E-Safety Mark is identified by a blue border.

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 aide-memoire 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 Self Review Tool. 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 documents and resources

South West Grid for Learning: www.swgfl.org.uk/Staying-Safe
The site contains a wide range of policy documents, resources and links to other sites.

School E-Safety Policy Templates: www.swgfl.org.uk/Policy

Digital Literacy and Citizenship Curriculum: www.swgfl.org.uk/DigitalLiteracy

SWGfL BOOST – A comprehensive e-safety support service for schools that includes an anonymous reporting tool, an incident response tool, an online reputation tool and online presentations and training: www.swgfl.org.uk/Boost

UK Safer Internet Centre: www.saferinternet.org.uk

Further links to documents and resources can be found on the review page for each aspect in the online tool: www.360safescotland.org.uk

Acknowledgements

South West Grid for Learning Trust would like to acknowledge the work of the SWGfL E-Safety Group who have been responsible for the production of the 360 degree safe e-safety self review tool.

Every effort has been made to ensure that the information included in this document is accurate. However, SWGfL can not guarantee it’s accuracy, nor can it accept liability in respect of the use of the material.

Element 1 / 4 This element reflects the importance of having a clear vision and strategy for e-safety, with effective policies and leadership. This should be owned and understood by all stakeholders. There should be effective self evaluation, monitoring, reporting systems and sanctions.

Policy & Leadership > Responsibilities

Use this self review tool to establish where your school is on the journey towards an effective e-safety strategy. Additional support material, resources and links to other websites are available on the SWGfL website: www.swgfl.org.uk

Element A	Policy and Leadership					What Evidence could you use?
Strand 1	Responsibilities					
	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	
Aspect 1 E-Safety Group	There is no e-safety group	The school is in the process of establishing an e-safety group	The school has an e-safety group with staff representation and a clear brief	The school has an active e-safety group with wide representation from the senior leadership team, staff (including Child Protection coordinator), parents and children/ young people. It has clear lines of responsibility and accountability.	The school has an active e-safety group with wide representation from within the school, for example, senior leadership team, teaching and support staff (including Child Protection coordinator), parents and carers, children / young people and the wider community. It has clear lines of responsibility and accountability which are understood by all members of the school. The group is actively integrated and collaborating with other relevant groups in school.	School vision and aims School improvement plan Self evaluation documents Job descriptions Minutes of meetings of relevant groups, and committees, including E-Safety Group and Parent Council E-Safety group terms of reference Incident logs and monitoring reports
Aspect 2 E-Safety Responsibilities	No one has responsibility for e-safety across the school	One or more members of staff have responsibility for e-safety, but there is little coordination of their work	The school has a designated E-Safety Coordinator / Officer with clear responsibilities.	The school has a designated E-Safety Coordinator / Officer with clear responsibilities. These include leadership of the e-safety group, professional learning and awareness. Designated persons are responsible for monitoring incidents and handling sensitive issues (including Child Protection). Many staff take responsibility for e-safety.	The school has a designated E-Safety Coordinator / Officer with clear responsibilities. These include leadership of the e-safety group, professional learning and awareness, and commitment to and coordination of an e-safety programme with the wider community. Designated persons are responsible for monitoring incidents and handling sensitive issues. All staff take active responsibility for e-safety.	

Element 1 / 4

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

Policy & Leadership > Policies

Use this self review tool to establish where your school is on the journey towards an effective e-safety strategy. Additional support material, resources and links to other websites are available on the SWGfL website: www.swgfl.org.uk

Element A — Policy and Leadership

Strand 2 — Policies

	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	What Evidence could you use?
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 effective and meets the school's responsibilities for the care and welfare of children. This may also reflect local or national guidelines / requirements.	The school has an e-safety policy, which is effective and meets the school's responsibility for the care and protection of children and young people. It has been developed in consultation with a wide range of staff and children / young people. There is "whole school ownership" of the policy. The policy is reviewed regularly (preferably annually).	The school has an e-safety policy, which is effective and meets the school's responsibilities for the care and protection of children. It has been developed in consultation with the staff, children and young people, 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 e-safety incidents. The policy is an integral part of School Improvement Planning.	E-Safety policy School improvement plan Minutes of the E-Safety Committee / other groups. Information for parents – letters, AUA, newsletter, website etc Home-school agreements Acceptable use policies (signed) Induction policies and procedures Feedback from staff Parent council minutes
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 computing systems, equipment and software in school.	The e-safety policy covers the use of the computing systems, equipment and software in school. It also covers the use of school-owned technology outside school and the use of personal technology in school. It is comprehensive in that it includes sections on issues such as social networking, cyber-bullying, data protection, passwords, filtering, digital and video images and use of mobile devices. The policy clearly states the school's commitment to working with parents / carers and children / young people to resolve e-safety incidents outside the school. It is clearly linked to positive behaviour policies and approaches, and the school's approach to ensuring the safety and well-being of staff and children/young people.	The e-safety policy covers the use of the computing systems, equipment and software in school. It also covers the use of school-owned technology outside school and the use of personal technology in school. It is comprehensive in that it includes sections on issues such as social networking, cyber-bullying, data protection, passwords, filtering, digital and video images and use of mobile and / or gaming devices. The policy is underpinned by the school's ethos and overall approach to health and wellbeing, with specific reference to policies on positive relations and behaviour. The policy clearly states the school's commitment to address with children/ young people the risks and responsibilities of e-safety out of school and to working with parents /carers, children / young people to resolve out-of-school incidents. The policy is clearly linked to the school's approach to working with other agencies to protect children through the GIRFEC practice model. The e-safety policy is differentiated and age related, in that it recognises the needs of young people at different ages and stages within the school.	

360safe School E-Safety Self Review Tool

A3

The Scottish Government
Riaghaltas na h-Alba

Element 1 / 4 This element reflects the importance of having a clear vision and strategy for e-safety, with effective policies and leadership. This should be owned and understood by all stakeholders. There should be effective self evaluation, monitoring, reporting systems and sanctions.

Policy & Leadership > Policies

Use this self review tool to establish where your school is on the journey towards an effective e-safety strategy. Additional support material, resources and links to other websites are available on the SWGfL website: www.swgfl.org.uk

Element A — Policy and Leadership

Strand 2 — Policies

	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	What Evidence could you use?
Aspect 3 Acceptable Use Agreement (AUA)	There are no Acceptable Use Agreements	Acceptable Use Agreements are being developed	Acceptable Use Agreements are in place for pupils / students and staff / volunteers.	Acceptable Use Agreements are in place for, and are acknowledged (or signed) by children / young people (as appropriate by age) and staff / adult volunteers. Children / young people have gone over the agreement with a teacher and fully understand what it means. Parents receive and acknowledge (or countersign) copies of the children / young people's Acceptable Use Agreement. There are clear induction policies to ensure that young people and adults who are new to the school are informed of and required to acknowledge (or sign) Acceptable Use Agreements.	Acceptable Use Agreements, which are differentiated by age and stage, are in place for, and are acknowledged (or signed) annually by, children / young people, staff /adult volunteers and community users. Parents receive and, annually, acknowledge (or countersign) copies of the children / young people's AUA. The clear induction policies ensure that young people and adults who are new to the school are informed of and required to sign AUAs. All users have knowledge of the e-safety policy and AUA and understand their responsibilities, as described in the policy.	E-Safety policy School improvement plan Minutes of the E-Safety Group / other groups. Information for parents – letters, AUA, newsletter, website etc Home-school agreements Acceptable Use agreement Induction policies and procedures Interviews with staff, parents, children and young people EA and other external reviews Department and faculty self-evaluation reports
Aspect 4 Self Evaluation	E-safety is not considered in the school's wider self-evaluation processes, for example departmental reviews, thematic reviews, reviews/ support visits carried out by Quality Improvement Officers from the Education Authority, and the school's regular cycle of self-evaluation using suitable Quality Indicators.	The school has begun to consider e-safety within the school's wider self-evaluation processes, for example departmental reviews, thematic reviews, reviews/ support visits carried out by Quality Improvement Officers from the Education Authority. E-safety is not yet fully embedded in the school's regular cycle of self-evaluation using suitable Quality Indicators	The school's wider self-evaluation processes address e-safety. There is reference to e-safety in documents such as departmental self-evaluation, EA reviews, and the school's regular cycle of self-evaluation using Quality Indicators. The school has identified and acknowledged some areas of strength, areas for development and priorities for action.	E-safety is a well embedded in the school's wider self-evaluation processes. Documents such as departmental / faculty self-evaluation reports, EA reviews and support / review visits from Quality Improvement Officers clearly acknowledge areas of strength and weakness and priorities for action. E-safety is included in the self-evaluation of personal support and child protection. The school has made use of children / young people and parent / carer surveys in identification of strengths, areas for development and priorities.	E-safety is a strong feature within the school's wider self-evaluation processes. Documents such as reports from departmental / faculty self-evaluation, EA reviews, self-evaluation of ICT, personal support and child protection processes clearly acknowledge strengths and areas for development and priorities for action. The school has made use children / young people, parent / carer and community user surveys in identification of strengths, areas for development and priorities. The school openly celebrates its e-safety successes in its wider self-evaluation processes.	

Element 1 / 4 This element reflects the importance of having a clear vision and strategy for e-safety, with effective policies and leadership. This should be owned and understood by all stakeholders. There should be effective self evaluation, monitoring, reporting systems and sanctions.

Policy & Leadership > Policies

Use this self review tool to establish where your school is on the journey towards an effective e-safety strategy. Additional support material, resources and links to other websites are available on the SWGfL website: www.swgfl.org.uk

Element A	Policy and Leadership					What Evidence could you use?
Strand 2	Policies					
	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	
Aspect 5 Whole School	E-safety is not referred to in other whole school policies.	The school is beginning to link e-safety into other whole school policies.	E-Safety is referred to in other whole school policies. These include policies on Positive Relationships and Behaviour, and anti-bullying, Child Protection and GIRFEC and whole school advice on Technologies and Health and Wellbeing.	There are clear and consistent links between the school e-safety policy and sections of other policies where there is reference to e-safety, for example, policies on Positive Relationships and Behaviour, and anti-bullying, Child Protection and GIRFEC and whole school guidance on Technologies and Health and Wellbeing. Learning and teaching policies include advice on making best use of digital technology, while adhering to e-safety policy.	E-safety is embedded in all relevant whole school policies. The school has carefully considered its approach to e-safety and provides a consistent e-safety 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 e-safety within such policies on Positive Relationships and Behaviour, anti-bullying, Child Protection and GIRFEC and whole school guidance on Technologies and Health and Wellbeing.	Self-evaluation on reports/reviews LA and other external reviews Acceptable user agreement Team and department self evaluation Surveys Whole school policies eg Anti-bullying, child protection / Safeguarding ICT / Positive relationships and behaviour / GIRFEC Whole school advice on technologies, health & wellbeing and learning & teaching Strategies for encouraging safe & responsible use on screen messages
Aspect 6 Developing A Culture of Safe and Responsible Use	There are no strategies or clear guidance on safe and responsible use.	There are a range of strategies for developing safe and responsible use, but these are not linked to an agreed policy / acceptable use agreement and are not consistently enforced.	Strategies for developing safe and responsible use are clearly stated in the e-safety policy and related policies on behaviour and anti-bullying. Users are aware of these strategies.	Strategies for developing responsible use are clearly stated in the e-safety policy and are consistent with those in related policies, for example, behaviour and anti-bullying. Staff have been part of the decision making process about strategies, such as restorative and solution-focused practice, and understand their importance. The school acknowledges and rewards positive use. Users understand that strategies agreed in the policy can be helpful to e-safety usage out of school and that incidents, such as cyber-bullying will be addressed by school and parents together.	Strategies for developing safe and responsible use of online communications technologies, including mobile phones and other devices brought to school by children/young people are clearly stated in the e-safety policy and are consistent with those in related policies, for example, positive relationships and behaviour and anti-bullying. The school has an inclusive approach to developing strategies, consulting all members of the school community. Users understand the importance of the strategies and few users fail to display safe and responsible use. The school acknowledges and rewards positive use. Users understand that the school's agreed strategies will help them in their out of school usage and that e-safety incidents that take place out of school will be addressed by school and parents together, if they are related to school (for example cyber-bullying). The school is strict in monitoring and applying the e-safety policy and a differentiated and appropriate range of strategies, though the attitudes and behaviour of users are generally positive.	

School E-Safety Self Review Tool

A5

The Scottish Government
Riaghaltas na h-Alba

Element 1 / 4 This element reflects the importance of having a clear vision and strategy for e-safety, with effective policies and leadership. This should be owned and understood by all stakeholders. There should be effective self evaluation, monitoring, reporting systems and sanctions.

Policy & Leadership > Policies

Use this self review tool to establish where your school is on the journey towards an effective e-safety strategy. Additional support material, resources and links to other websites are available on the SWGfL website: www.swgfl.org.uk

Element A	Policy and Leadership					What Evidence could you use?
Strand 2	Policies					
	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	
Aspect 7 Reporting Issues of E-Safety Misuse and Abuse	Users are unclear about their responsibilities to report e-safety incidents and there is no clear process for reporting misuse and abuse.	Systems and processes are in place for users to report e-safety incidents and abuse. These are not yet consistently understood nor consistently used.	Users understand their responsibilities to report e-safety incidents. They know and understand that there are clear systems for reporting abuse and understand that the processes must be followed rigorously. There are clear escalation processes for the handling of incidents. Reports are logged for future auditing / monitoring. Users have an understanding of how to report issues online, including to PoliceScotland and CEOP. There are systems in place to ensure feedback to person who raised initial concern.	Users understand their responsibilities to report e-safety incidents. They know, understand and use clear systems for reporting abuse and understand that processes must be followed rigorously. More than one reporting route is made available. Reports are logged and regularly audited and monitored. There are clear escalation processes for the handling of incidents. Users are confident that they can approach responsible persons if they have worries about actual, potential or perceived e-safety incidents. The school actively seeks support from other support agencies (for example local authority and regional broadband grid) in dealing with e-safety issues. Reports are logged for future auditing / monitoring. Users have an understanding of how to report issues online, including to Police Scotland and CEOP. There are systems in place to ensure feedback to person who raised initial concern	There are clearly known and understood systems for reporting e-safety incidents. The culture of the school encourages all members of the school and its wider community to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes. Reports are logged and regularly audited and monitored. The school actively seeks support from other support agencies (for example, the local authority social work team and the Child Protection Committee) in dealing with e-safety issues. There are good links with outside agencies, for example, the police, who can help the school and members of the community in dealing with these issues. School reporting contributes to a better understanding of online safety issues within the local area.	Behaviour and anti-bullying policies Rewards and sanctions policies Posters in classrooms / on-screen messages AUAs Incident logs with evidence of monitoring and auditing. Communications with external agencies

A6

Element 1 / 4

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

Policy & Leadership > Communications and Communications Technologies

Use this self review tool to establish where your school is on the journey towards an effective e-safety strategy. Additional support material, resources and links to other websites are available on the SWGfL website: www.swgfl.org.uk

Element A — Policy and Leadership

Strand 3 — Communications and Communications Technologies

	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	What Evidence could you use?
Aspect 1 Mobile Devices	There is no policy relating to the use of mobile devices and the school has not in any way addressed issues related to mobile devices.	A policy relating to the use of mobile devices is being developed, taking account of the views of staff, parents, children and young people and local and national guidance.	The school has a policy relating to the use of mobile devices. This has been developed in partnership with stakeholders, agreed by the school community and implemented. Plans are in place to review the implementation and impact of the policy.	The school has clearly understood and accepted policies relating to the use of mobile devices. Users understand the risks associated with the use of these devices and are encouraged to be responsible users, both inside school and outside school. Users understand digital citizenship and can describe what this means for online communication and relationships.	The school has clearly understood and accepted policies relating to the use of mobile devices. Users have a mature approach to their safe use. The school has realised the educational potential of these devices and has allowed / encouraged their safe use within school, where this is relevant and age appropriate to learning. Policies clearly set out how the school will respond to incidents of misuse. The school has consulted with parents and the wider community and gained their support for this policy.	Acceptable Use Agreements Home-school agreements Policy for the use of mobile devices Consultation with parents / surveys BYOD policy Teachers’ plans and curricular guidance

Element 1 / 4 This element reflects the importance of having a clear vision and strategy for e-safety, with effective policies and leadership. This should be owned and understood by all stakeholders. There should be effective self evaluation, monitoring, reporting systems and sanctions.

Policy & Leadership > Communications and Communications Technologies

Use this self review tool to establish where your school is on the journey towards an effective e-safety strategy. Additional support material, resources and links to other websites are available on the SWGfL website: www.swgfl.org.uk

Element A Policy and Leadership

Strand 3 Communications and Communications Technologies

	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	What Evidence could you use?
Aspect 2 Social Media	There is no policy relating to the use of social media.	A policy relating to the use of social media is being developed. Staff, parents/ carers and children and young people have been involved and their views considered.	The school has a policy relating to the use of social media. Users understand the policy, know what their responsibilities are within the policy, and are aware of the arrangements for monitoring the policy.	The school has clearly understood and accepted policies relating to the use, by staff and children / young people, of social media. The school values the educational potential of social media and is investigating how they might be used safely in school. Users are encouraged to be responsible users, both inside school and outside school. They understand digital citizenship, and are developing behaviours online which reflect that understanding, for example demonstrating respect for others. They understand the risks associated with the use of social media and are encouraged to talk about any worries or concerns they have about experiences online.	The school has clearly understood and accepted policies relating to the use of social media. The school values the educational potential of social media and encourages their safe use within school, where this is relevant and age appropriate to learning. The agreed policy outlines the establishment's approach to educating children and young people to become responsible digital citizens. Users understand the risks associated with the use of these systems, and are confident that they can protect themselves and respect others. They understand the concept of digital citizenship, and the associated rights and responsibilities. They talk openly to school staff or their parents about concerns they have about their experiences online or concerns about their friends. Users understand that use of these systems will be regularly monitored, with findings reported to the e-safety group. The school's response to misuse is clearly set out and is applied consistently. The school has developed the policy in partnership with staff, parents and children and young people and this process has ensured understanding of and commitment to the policy.	Acceptable Use Agreements Home-school agreements Policy for the use of mobile devices Consultation with parents / surveys Teachers' plans and curricular guidance Policy statements on using social media responsibly Minutes of working groups for use of social media

360safe School E-Safety Self Review Tool

A8

The Scottish Government
Riaghaltas na h-Alba

Element 1 / 4 This element reflects the importance of having a clear vision and strategy for e-safety, with effective policies and leadership. This should be owned and understood by all stakeholders. There should be effective self evaluation, monitoring, reporting systems and sanctions.

Policy & Leadership > Communications and Communications Technologies

Use this self review tool to establish where your school is on the journey towards an effective e-safety strategy. Additional support material, resources and links to other websites are available on the SWGfL website: www.swgfl.org.uk

Element A Policy and Leadership

Strand 3 Communications and Communications Technologies

	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	What Evidence could you use?
Aspect 3 Digital and Video Images	There are minimal arrangements for parental consent for using digital and video images, but no wider policy relating to their use.	A policy relating to the use and publication of digital and video images is being developed in partnership with stakeholders.	The school has appropriate policies relating to the use and publication of digital and video images which are understood by all and fully implemented. Parental permission is sought, as required in line with the policy. The policies are integrated into overarching policy on e-safety and linked to policies on learning and teaching and child protection.	The school has clearly understood and accepted policies relating to the use and publication of digital and video images. Parental permissions are gained when publishing personal images on the website or other publications. All members of the school understand their rights and responsibilities in the taking, use, sharing, publication and distribution of images. In particular children and young people understand how to protect themselves and respect others in relation to digital images and do not put themselves at risk or abuse others. Digital images are securely stored and disposed, in accordance with the Data Protection Act.	The school has clearly understood and accepted policies relating to the use and publication of digital and video images. Parental permissions are gained when publishing personal images on the website or other publications. All members of the school understand their rights and responsibilities in the taking, use, sharing, publication and distribution of images (and in particular the risks attached). Digital images are securely stored and disposed, in accordance with the Data Protection Act. Members of the school are encouraged to use digital and video images to evaluate and promote the quality of their teaching and learning, but also understand their responsibilities for any images they use.	Policy for the use of digital and video images Acceptable use agreements Newsletters, website, learning platform, VLE Schemes of work and lesson plans Learning and teaching policies Curricular guidance and lesson plans School's GLOW network
Aspect 4 Public Online Communications	There is no reference to e-safety on the school's website, learning platform, online newsletters etc	There are limited references to e-safety on the school's website, learning platform, online newsletters etc	The school's public online communications are used to provide information about e-safety. The school ensures safe practice when publishing information through these media.	The school's public online communications are used to provide information about e-safety. The school celebrates its successes in this field. The school ensures that good practice has been observed in the use of these media, for example, use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is no risk to members of the school community, through such publications.	The school's public online communications are used to provide information about e-safety. The school celebrates its successes in this field. The school ensures that good practice has been observed in the use of these media for example use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is no risk to members of the school community, through such publications. It addresses issues relevant to the e-safety of members of the wider community. These policies and practices are regularly reviewed and reinforced. Care is taken to assess e-safety in the use of new communication technologies.	

Element 1 / 4 This element reflects the importance of having a clear vision and strategy for e-safety, with effective policies and leadership. This should be owned and understood by all stakeholders. There should be effective self evaluation, monitoring, reporting systems and sanctions.

Policy & Leadership > Communications and Communications Technologies

Use this self review tool to establish where your school is on the journey towards an effective e-safety strategy. Additional support material, resources and links to other websites are available on the SWGfL website: www.swgfl.org.uk

Element A	Policy and Leadership					What Evidence could you use?
Strand 3	Communications and Communications Technologies					
	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	
Aspect 5 Professional Standards	The school has no policies or protocols in place for the use of new technologies for communications between the 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 staff and other members of the school and wider community.	In consultation with the staff, the school has in place policies and protocols for the use of new technologies for communications between the staff and other members of the school and wider community. Teaching staff follow the relevant GTCS Professional Standards for Registration, the Code of Professionalism and Conduct, and other national guidance on emerging technologies in schools. They know how to use digital technologies competently to enhance teaching and learning. 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 staff and other members of the school and wider community. Staff follow the relevant Professional Standards, the Code of Professionalism and Conduct and other national guidance about these technologies. Members of staff understand the need for communication with young people, parents / carers and members of the community to take place only through official school systems (for example school email, VLE etc) and that the communications must be professional in nature.	In consultation with the staff, the school has in place policies and protocols for the use of new technologies for communications between the staff and other members of the school and wider community. Staff follow the relevant Professional Standards and Code of Conduct and other national guidance about these technologies. Members of staff only use official school systems (for example school email, GLOW and other VLE etc.) for communication with young people, parents / carers and members of the community. Monitoring shows 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 e-safety issues have been carefully considered and policies updated before they are adopted for use.	Policy documents Staff handbooks Interviews with teachers Log of reported incidents and disciplinary actions

Element 2 / 4 This element reflects the importance of having effective systems in place to ensure the security of the school's computer 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.

Infrastructure > Passwords

Use this self review tool to establish where your school is on the journey towards an effective e-safety strategy.
Additional support material, resources and links to other websites are available on the SWGfL website: www.swgfl.org.uk

Element B	Infrastructure					What Evidence could you use?
Strand 1	Passwords					
	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	
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 local or national guidelines / requirements.	All users have clearly defined access rights to school systems. The school has clearly understood and accepted policies relating to the use of passwords. Passwords are secure and are consistent with local or national guidelines / requirements. Passwords are age appropriate and changed regularly. There are clear procedures for the provision of new passwords, with forced changes at first log-in. There are clear policies for the use and control of the "master / administrator" passwords	All users have clearly defined access rights to school systems. The school has clearly understood and accepted policies relating to the use of passwords. Passwords are secure and are consistent with local or national guidelines / requirements. Passwords are age appropriate and changed regularly. There are clear procedures for the provision of new passwords, with forced changes at first log-in. There are clear policies for the use and control of the "master / administrator" passwords. There are regular audits of user log ins to check for anonymous or unauthorised log ins. There is regular testing of systems to ensure that the password security policy is being correctly implemented.	Password security policy Logs and audits Home-school agreement Staff Handbooks Acceptable Use agreements

Element 2 / 4

This element reflects the importance of having effective systems in place to ensure the security of the school's computer 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.

Infrastructure > Services

Use this self review tool to establish where your school is on the journey towards an effective e-safety strategy.
Additional support material, resources and links to other websites are available on the SWGfL website: www.swgfl.org.uk

Element B	Infrastructure					What Evidence could you use?
Strand 2	Services					
	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	
Aspect 1 Connectivity and Filtering	The school has no filtering policy in place. Filtering is neither managed nor monitored.	A policy is in place for all users, but the filtering is neither regularly monitored nor updated. Illegal content (child sexual abuse images) is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list.	Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.	Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.	Internet access is filtered for all users. Differentiated internet access is available for staff and age appropriate access for children/ young people. Customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Content lists are regularly updated and internet use is logged and frequently monitored. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice. Pro-active monitoring alerts the school to breaches of the filtering or Acceptable Use policy, allowing rapid response. There is a clear route for reporting and managing changes to the filtering system. The school monitors content on its network to complement the filtering. There is an appropriate and balanced approach to providing access to online content.	Filtering Policy Monitoring logs and audits Review documents (internal and external) Acceptable Use agreements
Aspect 2 Technical Security	The school does not meet the e-safety technical requirements outlined in local or national guidelines / requirements	The school meets the e-safety technical requirements outlined in local or national guidelines / requirements.	The school meets the e-safety technical requirements outlined in local or national guidelines / requirements. There are regular reviews and audits of the safety and security of school computer systems.	The school meets the e-safety technical requirements outlined in local or national guidelines / requirements. There are regular reviews and audits of the safety and security of school computer systems, with oversight from senior leaders and these have impact on policy and practice. The school's computer infrastructure is secure and is not open to misuse or malicious attack.	The school meets the e-safety technical requirements outlined in local or national guidelines. There are regular reviews and audits of the safety and security of school ICT systems with oversight from senior leaders and these have 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.	

School E-Safety Self Review Tool

B3

The Scottish Government
Riaghaltas na h-Alba

Element 2 / 4 This element reflects the importance of having effective systems in place to ensure the security of the school's computer 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.

Infrastructure > Services

Use this self review tool to establish where your school is on the journey towards an effective e-safety strategy.
Additional support material, resources and links to other websites are available on the SWGfL website: www.swgfl.org.uk

Element B — Infrastructure

Strand 2 — Services

	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	What Evidence could you use?
Aspect 3 Personal Data	There is no agreed policy on secure holding, handling and destroying of personal information in line with Data Protection Act 1998 and related guidance.	A Personal Data policy is being developed. The school is working toward meeting the requirements of the Data Protection Act in line with local authority guidance and procedures. Independent schools have policies meeting their requirements as data holders.	The school has a Personal Data policy. All staff know and understand their statutory obligations under the Data Protection Act to ensure the safe keeping of personal data, minimising the risk of its loss or misuse. Parents and carers are informed about their rights and about the use of personal data through the Privacy Notice in the school handbook. The school, in partnership with the local authority, has processes in place to manage Freedom of Information requests.	The school has a Personal Data policy. All staff know and understand their statutory obligations under the Data Protection Act to ensure the safe keeping of personal data, minimising the risk of its loss or misuse. Schools understand the right of anyone to request a copy of one's own personal data through a Subject Access Request (SAR). Clear policies about the secure handling, transfer and disposal of data (passwords, encryption, and removable media) are known, understood and adhered to by users. Parents and carers are informed about their rights and about the use of personal data through the Privacy Notice. Data protection is enhanced by the use of encryption and / or two factor authentication for the handling or transfer of sensitive data. A member of the senior leadership team has responsibility for oversight of data protection and the related risks and is aware of school and local authority responsibilities and procedures.	The school has a Personal Data policy. All staff know and understand their statutory obligations under the Data Protection Act to ensure the safe keeping of personal data, minimising the risk of its loss or misuse. All staff understand the rights of anyone to make a Subject Acess Request and recognise when one is being made. The school in partnership with the local authority has systems in place to ensure that a SAR can be met within the timescale laid out in legislation. Clear policies about the secure handling, transfer and disposal of data (passwords, encryption, and removable media) are known, understood and adhered to by users. Parents and carers are informed about their rights and about the use of personal data through the Privacy Notice in the school handbook or website. Data protection is enhanced by the use of encryption and / or two factor authentication for the handling or transfer of sensitive data. A member of the senior leadership team has responsibility for oversight of data protection and the related risks and is aware of school and local authority responsibilities and procedures. All protected data is clearly labelled with Impact Labels. There is a clear procedure in place for audit logs to be kept and for reporting, managing and recovering from information risk incidents	Personal Data Policy Fair Processing Notice Job descriptions

360safe School E-Safety Self Review Tool

C1

The Scottish Government
Riaghaltas na h-Alba

Element 3 / 4

This element 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 computer systems and mobile devices – both in school and in the wider community.

Education > Children and Young People

Use this self review tool to establish where your school is on the journey towards an effective e-safety strategy.
Additional support material, resources and links to other websites are available on the SWGfL website: www.swgfl.org.uk

Element C	Education					What Evidence could you use?
Strand 1	Children and Young People					
	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	
Aspect 1 E-Safety Education	There is no planned approach to delivering e-safety education.	A planned approach to e-safety education is being developed. in line with Curriculum for Excellence Technologies outcomes levels TCH 1-08a, TCH 2-08a and TCH 3-08a and taking account of Health and Wellbeing outcomes, (16a across all levels)	E-safety education is covered with all children and young people, either within a programme or integrated into broader Technology or Health and Wellbeing programmes. Children/young people are aware of e-safety issues and can recount how to stay safe online. They understand the risks of social networking sites and are developing confidence in protecting themselves and respecting others. A range of relevant e-safety resources are used. Children and young people are achieving relevant outcomes within Curriculum for Excellence technologies and HWB.	A planned e-safety education programme takes place through both discrete lessons and wider curriculum opportunities. The entitlement of children/young people in all year groups is met by a programme that is mapped and regularly reviewed. There is progression where lessons build on prior learning. There are opportunities to assess and evaluate learners' progress. The curriculum should reflect the wider personal, social and technical aspects of e-safety education, making use of a broad range of current and relevant resources. The teaching should ensure opportunities for open discussion about young people's experiences online, and develop a culture which is open and accepting so that children/young people can talk about experiences such as cyber-bullying. Children and young people are developing as digital citizens.	A planned e-safety education programme takes place and is fully embedded in all aspects of the curriculum in all years and in other school activities, including extended provision. The entitlement of children/young people in all year groups is met by a programme that is mapped, audited and regularly revised. There is progression where lessons build on prior learning. There are opportunities to assess and evaluate learners' progress. The curriculum reflects the wider personal, social and technical aspects of e-safety education and is aligned with standards in other curriculum areas. It makes use of a broad range of current and relevant resources including new technologies to deliver e-safety messages in an engaged and relevant way. Young people are themselves involved in e-safety education for example through peer mentoring and there is evidence of differentiation for learners / vulnerable groups. Children and young people demonstrate a secure understanding of how to protect themselves and respect others. They understand what it means to be a digital citizen and how this relates to roles and responsibilities in their school and community. They report experiences of cyber – bullying and encourage their friends to talk about difficult and negative experiences online. The school regularly evaluates the effectiveness and impact of e-safety programmes.	Lesson plans Classroom resources Learning Platform, VLE, website Work samples, exercise books etc Curricular guidance/ programmes

360safe

School E-Safety Self Review Tool

C2

The Scottish Government
Riaghaltas na h-Alba

Element 3 / 4

This element 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 computer systems and mobile devices – both in school and in the wider community.

Education > Children and Young People

Use this self review tool to establish where your school is on the journey towards an effective e-safety strategy.
Additional support material, resources and links to other websites are available on the SWGfL website: www.swgfl.org.uk

Element C	Education					What Evidence could you use?
Strand 1	Children and Young People					
	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	
Aspect 2 Digital Literacy	There are no opportunities for children/ young people to develop, nor practice, digital literacy skills.	Opportunities for children / young people to gain an understanding of digital literacy skills that reflect current pedagogical practice are being developed. This may include: critical thinking and evaluation, ability to find and select information and cultural / social understanding	Children/young people are taught in some lessons to be critically aware of the content they access on-line and how to validate the accuracy of information. They have an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. There is evidence that functional skills to operate online in a safe and appropriate way are taught. Children are developing skills in using digital technologies to extend their learning, to become more independent and to develop creativity.	Children/young people are beginning to operate effectively and safely in social media communities. They are aware of the need to protect themselves and respect others. They are becoming creative and use online technology to solve problems and find innovative approaches to learning. There are opportunities in a wide range of lessons for children / young people to be taught to be critically aware of the content they access on-line and how to validate the accuracy of information. Children / young people are aware of issues related to ownership, plagiarism and copyright across all media and understand the wider social and commercial context relating to their use of technology.	Children and young people are developing creativity and innovation, critical thinking and problem solving, and communication and collaboration skills through planned opportunities for developing digital literacy. They use social media to collaborate and can operate effectively and safely within those communities. Children and young people are taught in the majority of lessons to practice the skills of safe and discriminating online behaviour and know how to validate the accuracy of information. They acknowledge copyright and intellectual property rights in all their work. Children/young people understand the social and commercial implications of their use of technology and can communicate safely and appropriately with a range of different audiences in a variety of contexts. Digital literacy planning aligns with and complements e-safety education, ensuring that children and young people protect themselves and respect others.	Curriculum guidance and programmes Lesson plans Classroom resources Peer mentoring programmes Buddying schemes Contributions from children and young people in school assemblies, lesson publications, school website and at parents' evenings.
Aspect 3 The Contribution of Young People	The school does not acknowledge or use the skills and knowledge of young people in the use of new technologies in the development of its e-safety strategy.	The school is developing opportunities to acknowledge and use the skills and knowledge of young people in the use of new technologies in the development of its e-safety strategy.	The school acknowledges, learns from and uses the skills and knowledge of young people in the use of new technologies. These contribute to the development of its e-safety strategy, particularly the policy and education programmes.	The school acknowledges, learns from and uses the skills and knowledge of young people in the use of new technologies. These significantly inform school e-safety policy and programmes. The school involves children / young people in delivering its e-safety campaigns and in the support of peer groups. There are mechanisms to canvass children / young people for feedback and opinion.	The school acknowledges, learns from and uses the skills and knowledge of young people in the use of new technologies. These significantly inform school e-safety policy and programmes. The school involves children/young people in designing and delivering its e-safety campaigns. They support peer groups and provide a clear and effective reporting route. There are mechanisms to canvass feedback and opinion from children / young people. Young people actively contribute to parents' evenings and family learning programmes with e-safety as their focus.	

360safe

School E-Safety Self Review Tool

C3

The Scottish Government
Riaghaltas na h-Alba

Element 3 / 4 This element 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 computer systems and mobile devices – both in school and in the wider community.

Education > Staff

Use this self review tool to establish where your school is on the journey towards an effective e-safety strategy.
Additional support material, resources and links to other websites are available on the SWGfL website: www.swgfl.org.uk

Element C	Education					What Evidence could you use?
Strand 2	Staff					
	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	
Aspect 1 Professional Learning	There is no planned e-safety training programme for staff. Child Protection training does not include e-safety.	A planned e-safety staff training programme is being developed, which aligns with Child Protection training.	There is a planned programme of staff e-safety training that is regularly revisited and updated. There is clear alignment and consistency with other Child Protection training and vice versa. Training needs are informed through audits and the induction programme for new staff includes e-safety. There is evidence that key members of staff (for example E-Safety Officer, Child Protection Officer,) have received more specific training beyond general awareness raising. The E-Safety Officer can demonstrate how their own professional expertise has been sustained (for example through conferences, research, training or membership of expert groups.)	There is a planned programme of e-safety training for all staff that is regularly revisited and updated. There is clear alignment and consistency with other professional learning in Child Protection and vice versa. Training needs are informed through audits and the induction programme for new staff includes e-safety. Where relevant, e-safety training is included in PRD targets. There is evidence that key members of staff (for example E-Safety Officer, Child Protection Coordinator, Data Officer) have received more specific training beyond general awareness raising, some of which is accredited and recognised. The E-Safety Officer can demonstrate how their own professional expertise has been sustained and accredited.	There is a planned programme of e-safety training for all staff that is regularly revisited and updated and differentiated to need. The school takes every opportunity to research and understand current good practice and training reflects this. There is clear alignment and consistency with other Child Protection /GIRFEC training and vice versa. Training needs are informed through audits and the induction programme for new staff includes e-safety. Professional learning takes account of the Standard for Career-long Professional Learning. Where relevant, e-safety training is included in PRD targets. There is evidence that key members of staff (for example E-Safety Officer, Child Protection Coordinator, Data Officer) have received more specific training beyond general awareness raising, some of which is accredited and recognised. The E-Safety Officer can demonstrate how their own professional expertise has been sustained and accredited. The culture of the school ensures that staff support each other in sharing knowledge and good practice about e-safety. Staff are confident in their understanding of e-safety issues and their role in ensuring the safety and wellbeing of children and young people. Across the school community there is a developing understanding of digital citizenship. The impact of e-safety training is evaluated and informs subsequent practice.	Personal learning needs analysis Staff training programmes Personal learing portfolios Induction programmes Good practice visits / learning walks interviews with staff External accreditation.

Element 3 / 4

This element 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 computer systems and mobile devices – both in school and in the wider community.

Education > Parents and Carers

Use this self review tool to establish where your school is on the journey towards an effective e-safety strategy.
Additional support material, resources and links to other websites are available on the SWGfL website: www.swgfl.org.uk

Element C	Education					What Evidence could you use?
Strand 3	Parents and Carers					
	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	
Aspect 1 Parental Engagement	The school does not provide opportunities for parents to receive information or education about e-safety.	The school is developing opportunities for parents to receive information or education about e-safety and beginning to involve parents in discussion about these issues.	The school provides some opportunities for parents to receive information or education about e-safety. The school has run events / meetings for parents and carers and has referenced e-safety issues in communications (for example newsletter, website, and social media). Parents are aware of and have acknowledged the Acceptable Use Agreement for children/ young people. Parents have had opportunities to share with each other and the school their attitudes to e-safety and young people.	The school provides regular opportunities for parents to receive information or education about e-safety. There is evidence that parent e-safety events / communications are effective. There are clear routes for parents to report issues. Parents understand that e-safety is a joint responsibility between home and school. They are confident that the school can support them with online safety issues or signpost additional support and advice and that the school welcomes insights from their experience and expertise. Parents are aware of and have acknowledged the Acceptable Use Agreement for children/young people and there is clear evidence of support. Parents understand the links between e-safety and the school's positive relations and behaviour policy and anti-bullying policies.	The school provides regular opportunities for parents to receive information or education about e-safety. There is evidence that parent e-safety events / communications are effective. The school and parents and carers understand the importance of partnership and joint responsibility for e-safety education and in ensuring children are safe online, including where appropriate monitoring/ regulation of children's online contacts. There are clear routes for parents to report issues. Parents are confident that the school can support them with online safety issues or signpost additional support and advice and that they can support the school as appropriate when issues arise. Parents are aware of and have acknowledged the Children / Young People Acceptable Use Agreement and there is clear evidence of support. The school community, including parents, is developing an understanding of digital citizenship so that they can understand the links between roles and responsibilities in the school community and online communities. Parents and carers know about the school's complaints procedure and how to use it effectively. The school is effective in engaging "hard to reach" parents in e-safety programmes.	Acceptable Use agreements Letters to parents, newsletters, Website - e-safety section for parents / carers and the community Parents' evenings / courses Family learning events Interviews with parents, children, young people and staff

Element 4 / 4 This element reflects the importance of schools knowing how the effectiveness of their policies and practice is impacting on e-safety outcomes. Has the school considered how it will monitor and is monitoring embedded in practice?

Standards > Monitoring

Use this self review tool to establish where your school is on the journey towards an effective e-safety strategy.
Additional support material, resources and links to other websites are available on the SWGfL website: www.swgfl.org.uk

Element D	Standards					What Evidence could you use?
Strand 1	Monitoring					
	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	
Aspect 1 Monitoring and Reporting on E-Safety Incidents	There is no monitoring of e-safety incidents.	A process for the monitoring of e-safety incidents is being developed.	Monitoring of e-safety incidents takes place and records are kept, as part of the school's normal monitoring and recording processes (for example child protection / behaviour). The records are reviewed / audited and reported to the school's senior leaders. Parents are informed of e-safety incidents, as relevant.	Detailed monitoring of e-safety incidents takes place that includes: references to individual incidents within school; incidents beyond school as relevant and regular technical reports from system monitoring. Discrete records are kept and are reviewed / audited and reported to the school's senior leaders. Consistent repeated incidents and emerging trends are noted and investigated. There are clear systems for communicating incidents with the Parent Council and parents.	Detailed monitoring of e-safety incidents takes place that includes: references to individual incidents within school; incidents beyond school and regular technical reports from system monitoring. Discrete records are kept and are reviewed / audited and reported to the school's senior leaders and the Parent Council. There are clear systems for communicating incidents with parents. Patterns and trends are investigated and learning from reported incidents feeds back into practice and policy. The school actively cooperates with other agencies and the Child Protection/GIRFEC groups to help ensure the development of a consistent and effective local e-safety strategy. All parents / carers are informed of patterns of e-safety incidents as part of the school's e-safety awareness raising.	Incident logs and audits / reviews School Improvement Plan Self Evaluation documents Minutes of meetings of relevant groups, and committees, including parent council Monitoring reports
Aspect 2 Impact of the E-Safety Policy and Practice	The impact of the e-safety policy and practice is not evaluated	Systems to evaluate the impact of e-safety policy and practice are being developed.	The impact of the e-safety policy and practice is evaluated through the review of e-safety incident logs, behaviour logs, surveys of staff, young people / children, parents / carers.	The impact of the e-safety policy and practice is evaluated through the review of e-safety incident logs, behaviour logs, surveys of staff, young people / children, parents / carers. Children /young people can talk confidently about their responsibilities online, about the relationship between expectations of their behaviour online and in school. They understand the concept of digital citizenship. The school reviews the effectiveness of e-safety support received from external agencies. There is balanced professional debate about the evidence taken from the logs and the impact of preventative work for example e-safety education, awareness and training.	The impact of the e-safety policy and practice is evaluated through the review of e-safety incident logs, behaviour logs, surveys of staff, young people / children, parents / carers. Children and young people are confident in talking about their responsibilities online, about protecting themselves and respecting others and about digital citizenship. The school reviews the effectiveness of e-safety support received from external agencies. There is balanced professional debate about the evidence taken from the logs and the impact of preventative work for example e-safety education, awareness and training. Evidence from reports of incidents and discussion with children / young people indicates that through their increased knowledge they are more likely to report incidents of cyber-bullying and talk openly about concerns to school staff and parents. The evidence of impact is shared with other schools, agencies and CPC to help ensure the development of a consistent and effective local e-safety strategy.	

School E-Safety Self Review Tool

R1

Record Sheet 1

This record sheet should be used with the 360 degree safe 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.

Element A	Policy and Leadership						
	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	COMMENT	SOURCES OF EVIDENCE
Strand 1	**Responsibilities**						
Aspect 1 E-Safety Group							
Aspect 2 E-Safety Responsibilitie							
Strand 2	**Policies**						
Aspect 1 Policy Development							
Aspect 2 Policy Scope							
Aspect 3 Acceptable Use Agreement (AUA)							
Aspect 4 Self Evaluation							
Aspect 5 Whole School							
Aspect 6 Developing a Culture of Safe and Responsible Use							
Aspect 7 Reporting Issues of E-Safety Misuse and Abuse							

School E-Safety Self Review Tool

R2

Record Sheet 2

This record sheet should be used with the 360 degree safe 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.

Element A	Policy and Leadership						
	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	COMMENT	SOURCES OF EVIDENCE
Strand 3	Communications and Communications Technologies						
Aspect 1 Mobile Devices				▨			
Aspect 2 Social Media				▨			
Aspect 3 Digital and Video Images				▨			
Aspect 4 Public Online Communications				▨			
Aspect 5 Professional Standards				▨			
Element B	Infrastructure						
Strand 1	Passwords						
Aspect 1 Password Security			▨				
Strand 2	Services						
Aspect 1 Connectivity and Filtering				▨			
Aspect 2 Technical Security			▨				
Aspect 3 Personal Data			▨				

School E-Safety Self Review Tool

R3

Record Sheet 3

This record sheet should be used with the 360 degree safe 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.

Element C	**Education**						
	LEVEL 5	LEVEL 4	LEVEL 3	LEVEL 2	LEVEL 1	COMMENT	SOURCES OF EVIDENCE
Strand 1	**Children and Young People**						
Aspect 1 E-Safety Education				▨			
Aspect 2 Digital Literacy				▨			
Aspect 3 The Contribution of Young People				▨			
Strand 2	**Staff**						
Aspect 1 Professional Learning			▨				
Strand 3	**Parent and Carers**						
Aspect 1 Parental Engagement				▨			
Element D	**Standards and Inspection**						
Strand 1	**Monitoring**						
Aspect 1 Monitoring and Reporting on E-Safety Incidents			▨				
Aspect 2 Impact of the E-Safety Policy and Practice			▨				

Name of School:

Contact Person:

School Address:

Email Address:

Telephone Number: