School Online Safety Self-Review Tool

Updated February 2018

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter, EX2 5WS
Registered in England and Wales, Company Number 5589479. Charity Number 1120354. VAT Reg. Number 880 8618 88

Contents

Introduction

The development and expansion of the use of ICT / computing, and particularly of the internet, has transformed learning in schools. Children and young people will need to develop high level ICT / computing skills, not only to maximise 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 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 online 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 online 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 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 online safety policy and practice and provide:

- Management information and stimulus that can influence the production or review of online 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 online safety to practice that is aspirational and innovative.

The online Self Review Tool is available, free of charge to all schools at 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. It is, however, strongly recommended that schools should not use this pdf version alone – the online tool provides a more interactive and comprehensive method to review their online 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:

A. Policy & Leadership	B. Infrastructure	C. Education	D. Standards & Inspection

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 online safety policy and practice	Policy and practice is coherent and	Policy and practice is aspirational and

For each aspect, the benchmark level for the Online Safety Mark will have a light blue background like this.

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. 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

360 degree safe Online Tool
https://360safe.org.uk/

Access the online version of this tool and also access the help and other resources.

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

School Online Safety Policy Templates
https://swgfl.org.uk/OnlineSafetyPolicy

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

Online Safety BOOST
http://boost.swgfl.org.uk/
A comprehensive online safety support service for schools that includes an anonymous reporting tool, an incident response tool, an online reputation tool and online presentations and training.

360data
https://360data.org.uk/
A new addition to the 360 degree safe self review tools - 360data online data protection self-review tool allows you to review your data protection policies and practice.

UK Safer Internet Centre
https://saferinternet.org.uk/

Acknowledgements

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

Element A: Policy and Leadership

This element reflects the importance of having a clear vision and strategy for online 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 agreed responses to misuse.

Strand 1: Responsibilities

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

Aspect 1: Online Safety Group

This aspect describes how the school manages their online safety, strategy, involving a group with wide ranging representation.

	Level	Descriptor
Aspect 1: Online Safety Group	5	There is no online safety group
	4	The school is in the process of establishing an online safety group
	3	The school has an online safety group with staff representation and a clear brief
	2	The school has an active online 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.
	1	The school has an active online 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.

Aspect 2: Online Safety Responsibilities

This aspect describes the roles of those responsible for the school online safety strategy.

	Level	Descriptor
Aspect 2: Online Safety Responsibilities	5	No one has responsibility for online safety across the school
	4	One or more members of staff have responsibility for online safety, but there is little coordination of their work
	3	The school has designated and trained a member of staff responsible for online safety with clear responsibilities. These include leadership of the online safety group, professional learning and awareness.
	2	The school has designated a member of staff responsible for online safety with clear responsibilities. These include leadership of the online safety group, professional learning and awareness. They are responsible for monitoring incidents. They work closely with the person responsible for Child Protection. A number of staff members take an active role in online safety.
	1	The school has designated a member of staff responsible for online safety with clear responsibilities. These include leadership of the online safety group, staff training and awareness, commitment to and coordination of an online safety programme with the wider community. They are responsible for monitoring incidents and handling sensitive issues, working closely with the person responsible for Child Protection. All staff take active responsibility for online safety.

Strand 2: Policies

This strand allows schools/colleges to review whether they have in place effective structures for making and reviewing online safety policies, that online safety 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 online safety regarded as a whole school issue? Is online safety regarded as a welfare issue rather than simply a technical issue? Do users know how, and to whom, to report incidents? Are they confident they will be dealt with sympathetically and rigorously? Are responses to misuse clear, agreed and effective?

Aspect 1: Policy Development

This aspect describes the process of establishing an effective online safety policy: the stakeholders involved and their responsibilities; consultation, communication, review and impact.

	Level	Descriptor
Aspect 1: Policy Development	5	There is no online safety policy.
	4	The school is in the process of establishing an online safety policy.
	3	The school has an online safety policy, which is effective and meets the school's safeguarding obligations. This may also reflect local or national guidelines / requirements.
	2	The school has an online safety policy, where roles are clearly defined. It is effective and meets the school's and national child protection and safeguarding obligations. 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).
	1	The school has an online safety policy, where roles are clearly defined. It 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 / 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 online safety incidents. The policy is an integral part of school improvement planning.

Aspect 2: Policy Scope

This aspect considers policy content; its breadth in terms of technology and expectations around behaviour and its relevance to current social trends and educational developments.

	Level	Descriptor
Aspect 2: Policy Scope	5	There is no online safety policy.
	4	The school is in the process of establishing an online safety policy and exploring what it might include.
	3	The online safety policy is limited to the use of the computing systems, equipment and software in school.
	2	The online safety policy covers the use of the computing systems, equipment and software. 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 roles, on issues such as social networking, online bullying, data protection, passwords, filtering, digital and video images and use of mobile devices. It establishes school expectations regarding ethics and behaviour of all users.
	1	The online safety policy covers the use of the computing systems, equipment and software. 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 roles and issues such as social networking, online-bullying, data protection, passwords, filtering, digital and video images, extremism and use of mobile and / or gaming devices. It establishes school expectations regarding ethics and behaviour of all users. 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 is clearly linked to the school's approach to working with other agencies to protect children through the GIRFEC practice model. The online safety policy is differentiated and age related, in that it recognises the needs of young people at different ages and stages within the school.

Aspect 3: Acceptable Use

This aspect considers how a school communicates its expectations with all staff, learners and parents/carers for acceptable use of technology and the steps toward successfully implementing them in a school. This is supported by evidence of users' awareness of their responsibilities.

	Level	Descriptor
Aspect 3: Acceptable Use	5	There is no guidance for users on the acceptable use of technology
	4	Acceptable Use Policies are being developed in partnership with the appropriate local authority officer.
	3	Acceptable use policies are in place for all users of technology on the school site.
	2	Working together with the local authority officer responsible for the AUP, guidance on the acceptable use of technology is provided for all users of technology on the school site. Where school technology is used off site this should be covered in the AUP. These expectations are clearly and regularly communicated. The guidance is aligned with relevant existing policies and embedded within the culture of the school. Where AUPs are used, these may be acknowledged by children / young people or parents, where appropriate. It is clear to staff that acceptable use forms part of their contract. There are clear induction policies to ensure that anyone new to the school is informed of expectations of acceptable use.
	1	The school has worked together with the local authority officer responsible for the AUP to ensure guidance on the acceptable use of technology is provided for all users of technology on the school site. Where school technology is used off site this should be covered in the AUP. These expectations are clearly and regularly communicated. The guidance is aligned with relevant existing policies and embedded within the culture of the school. Where AUPs are used, these may be acknowledged by children / young people or parents, where appropriate. It is clear to staff that acceptable use forms part of their contract. There are clear induction policies to ensure anyone new to the school is informed of expectations of acceptable use. The guidance is regularly reviewed in the light of current practice legislation and changes in technology. There is a clear differentiation of acceptable use guidance according to age, role and need.

Aspect 4: Self Evaluation

This aspect describes how the online safety self-evaluation process builds on and aligns with other self-evaluation mechanisms the school might use.

	Level	Descriptor
Aspect 1: Online Safety Group	5	Online safety is not considered within school wider self-evaluation processes, for example departmental reviews, thematic reviews, reviews and performance reports, support / review visits from Quality Improvement Officers from the Local Authority, and the school's regular cycle of self-evaluation using suitable Quality Indicators.
	4	The school has begun to consider online safety within the school's wider self-evaluation processes, for example departmental reviews, thematic reviews, support visits / performance reports carried out by Quality Improvement Officers from the Local Authority. Online safety is not yet fully embedded in the school's regular cycle of self-evaluation using suitable Quality Indicators
	3	The school's wider self evaluation processes address online safety. There is reference to online safety in documents such as departmental self-evaluation, LA reviews and performance reports, 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.
	2	Online safety is a strong feature within the school's wider self-evaluation processes. Documents such as departmental / faculty self-evaluation reports, LA reviews and performance reports, support / review visits from Quality Improvement Officers clearly acknowledge areas of strength and weakness and priorities for action. Online 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. The school may be using review frameworks such as the Digital Schools Award for Scotland in preparation for quality mark submissions.
	1	Online safety is a strong feature within the school's wider self-evaluation processes. Documents such as reports from departmental / faculty self-evaluation, LA reviews and performance reports, self-evaluation of digital literacy, personal support and child protection processes clearly acknowledge strengths and areas for development and priorities for action. The school has made use of children / young people, parent / carer and community user surveys in identification of strengths, areas for development and priorities. The school may be using review frameworks such as the Digital Schools Award for Scotland in preparation for quality mark submissions. The school openly celebrates its online safety successes in its wider self-evaluation processes.

Aspect 5: Whole School

This aspect describes how the online safety policy is consistent with school expectations in other relevant policies and practices and vice versa e.g. behaviour, anti-bullying, Prevent action plan; PSE, child protection / safeguarding and computing policies. There is evidence that the policy is embedded across the school.

	Level	Descriptor
Aspect 5: Whole School	5	Online Safety is not referred to in other whole school policies
	4	Links are beginning to be made between online safety and other whole school policies and strategies. Awareness is being raised by the inclusion of these links.
	3	Online safety is referred to in a wide range of whole school policies and strategies. These are likely to include policies on Positive Relationships and Behaviour, the local authority's digital learning and teaching strategy (if applicable) and anti-bullying, Child Protection and GIRFEC. In addition whole school policy on Technologies and Health and Wellbeing and the Prevent Action Plan should be included.
	2	There are clear and consistent links between the online safety policy and sections of other policies and strategies where there is reference to online safety, for example, policies on Positive Relationships and Behaviour, the local authority's digital learning and teaching strategy (if applicable) and anti-bullying, Prevent, 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 online safety policy.
	1	Online safety is embedded in all relevant policies and strategies. The school has carefully considered its approach to online safety and provides a consistent online safety message to all members of the school community. This is achieved through a variety of media and activities that promote whole school input. This is particularly apparent in the references to online safety within such policies and strategies on Positive Relationships and Behaviour, and anti-bullying, Prevent, 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 the online safety policy.

Aspect 6: Developing a Culture of Safe and Responsible Use

This aspect considers the actions a school may take and the strategies it employs in response to misuse. Responsible use is acknowledged through celebration and reward.

	Level	Descriptor
Developing a Culture of Safe and Responsible Use	5	There are no strategies or clear guidance on safe and responsible use.
	4	There is a range of strategies for developing safe and responsible use, but these are not linked to an agreed acceptable use policy and are not consistently enforced.
	3	Strategies for developing safe and responsible use are clearly stated in the online safety policy and related policies on behaviour and anti-bullying. Users are aware of these strategies.
	2	Strategies for developing responsible use are clearly stated in the online safety policy and relevant school policies and users are aware of these strategies. Children / young people and staff have been part of the decision making process about strategies, through preventative work, restorative and solution-focused practice and understand their importance. The school acknowledges and rewards positive use. Strategies are regularly reviewed in the light of current practice and changes in technology.
	1	Strategies for developing responsible use are clearly stated in the online safety policy and relevant school policies and users are aware of these strategies. There is 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. Positive use is acknowledged and rewarded. Strategies are regularly reviewed in light of current practice and changes in technology. The school is rigorous in monitoring and applying the online safety policy and a differentiated and agreed range of strategies.

Aspect 7: Reporting Issues of Online Safety Misuse and Abuse

This aspect describes the routes and mechanisms the school provides to report abuse and misuse.

	Level	Descriptor
Reporting Issues of Online Safety Misuse and Abuse	5	Users are unclear about their responsibilities to report online safety incidents and there is no clear process for reporting misuse and abuse.
	4	Systems and processes are in place for users to report online safety incidents and abuse. These are not yet consistently understood nor consistently used.
	3	Users understand their responsibilities to report online safety incidents. They know and understand that there are clear systems for reporting abuse and understand that the processes will be followed rigorously. There are agreed 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 Police Scotland and CEOP. There are systems in place to ensure feedback to person who raised initial concern.
	2	Users understand their responsibilities to report online safety incidents. They know, understand and use clear systems for reporting abuse and understand that processes will be followed rigorously. More than one reporting route is made available. There are agreed escalation processes for handling incidents. Reports are logged and regularly audited and monitored. Users are confident that they can approach responsible persons if they have worries about actual, potential or perceived online safety incidents. The school actively seeks support from other support agencies (for example local authority and/or Police Scotland and CEOP) for online safety issues. Reports are logged for future auditing / monitoring. There are clear policies in place to report online safety incidents in line with local safeguarding arrangements. There are systems in place to ensure feedback to person who raised initial concern.
	1	There are clearly known and understood systems for reporting online safety incidents. The culture of the school encourages all members of the school 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 online 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.

Strand 3: Communications and Communications Technologies

This strand allows schools to consider whether the online safety aspects related to the use of a wide range of digital technologies has been sufficiently considered in wider policies and practice.

Has the school considered how they will ensure the safe use of digital devices as they become more and more prevalent in learning and teaching? Has the school encouraged professional debate and understanding about the use of these technologies?

Aspect 1: Mobile Technology

This aspect considers the effective management of mobile devices, apps and services and the implementation of an effective safeguarding strategy. This includes not only school provided technology, but also personal technology, e.g. bring your own device (BYOD).

	Level	Descriptor
Aspect 1: Policy Development	5	There is no policy relating to the use of mobile devices.
	4	An acceptable use policy relating to the use of mobile technology is being developed and is in the process of being implemented.
	3	The school has an acceptable use policy relating to the use of mobile technology (where applicable to school or personal devices) that covers use by staff, visitors and children / young people.
	2	The school has a clearly understood and accepted policy relating to the use of mobile technology (where applicable to school or personal devices) that covers use by staff, visitors and children / young people. Mechanisms are in place to monitor and intervene when issues arise. Users understand the risks associated with the use of mobile technology and are encouraged to be responsible users, both in school and beyond. Where the use of personal technology, e.g. BYOD, is encouraged there is clear guidance.
	1	The school has a clearly understood and accepted policy relating to the use of mobile technology (where applicable to school or personal devices) that covers use by staff, visitors and children / young people. Mechanisms are in place to monitor and intervene when issues arise. Users understand the risks associated with the use of mobile technology and are encouraged to be responsible users, both in school and beyond. There are clear expectations for the use of mobile technology, including BYOD, where appropriate. The school has consulted with parents and the wider community and gained their support for this policy.

Aspect 2: Social Media

This aspect covers the use of social media in, by and, where appropriate, beyond the school. It considers how the school can educate all users about responsible use of social media.

	Level	Descriptor
Aspect 2: Social Media	5	There is no policy relating to the use of social media and no planned programme of education.
	4	A policy relating to the use of social media and a planned programme of education is being developed.
	3	The school has worked with the local authority to develop a policy relating to the use of social media and users understand that, where applicable, use of these systems may be monitored and content moderated. The policy clearly references a planned programme of education relating to the safe and appropriate use of social media. The school is aware of the impact of social media comments made about it by others.
	2	The school has worked with the local authority to develop clearly understood and accepted policies relating to the use, by children / young people, staff and other users of social media. The policy clearly references a planned programme of education relating to the safe and appropriate use of social media. Users understand that, where applicable, use of these systems may be monitored and content moderated. Users understand the risks associated with the use of social media and are encouraged to be responsible users, both inside school and beyond. The school understands the impact of social media comments about both the school and its community and has begun to implement agreed responses where necessary.
	1	The school has worked with the local authority to develop clearly understood and accepted policies relating to the use of social media. The policy clearly references a planned programme of education relating to the safe and appropriate use of digital technology. Users understand that, where applicable, use of these systems may be monitored and content moderated. Users understand the risks associated with the use of social media and are encouraged to be responsible users, both inside school and beyond. The school has consulted with parents and the wider community and gained their support for this policy. The school is able to respond effectively to social media comments made by others. Lessons on safe and responsible use of social technologies are embedded as part of a wider online safety programme and are supported by active engagement with parents/carers and the school community.

Aspect 3: Digital and Video Images

This aspect describes how the school manages the use and publication of digital and video images in relation to the requirements of current data protection legislation.

	Level	Descriptor
Aspect 1: Policy Development	5	There is no policy relating to the use and publication of digital and video images.
	4	A strategy to ensure alignment with the local authority policy relating to the use and publication of digital and video images is being developed in partnership with stakeholders.
	3	The school has a strategy to ensure it aligns with the local authority's policy relating to the use and publication of digital and video images and parental permission is sought, as required. The strategy also references the use of digital images by children / young people as part of their learning. The strategy is integrated into overarching online safety policy and linked to policies on learning and teaching and child protection
	2	The school has a clearly understood and accepted strategy to ensure alignment with the local authority's policy on 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 current data protection legislation.
	1	The school has clearly understood and accepted strategy to ensure it aligns with the local authority's policy 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 current data protection legislation. The strategy is differentiated so that it is relevant to the ages, stages and maturity of the children / young people - recognising the personal rights of older children / young people over images of themselves.

Aspect 4: Public Online Communications

This aspect describes how the school manages its public facing online communications, both in managing risk and disseminating online safety advice, information and practice.

	Level	Descriptor
Aspect 4: Public Online Communications	5	There is no reference to online safety on the school's website, learning platform, social media, online newsletters etc.
	4	There are only limited references to online safety on the school's website, learning platform, social media, online newsletters etc.
	3	The school's public online communications are used to provide information about online safety. The school ensures safe practice when publishing information through these media.
	2	The school's public online communications are used to provide information about online safety. The school celebrates its successes in this field and ensures that good practice has been observed in the use of these media e.g. use of digital and video images, copyright, identification of young people, publication of calendars and personal information – ensuring that there is minimal risk to members of the school community, through such publications.
	1	The school's public online communications are used to provide information about online safety. The school celebrates its successes in this field and ensures that good practice has been observed in the use of these media e.g. use of digital and video images, copyright, identification of young people, publication of calendars and personal information – ensuring that there is minimal risk to members of the school community, through such publications. These policies and practices are regularly reviewed and reinforced. Care is taken to assess online safety in the use of new communication technologies.

Aspect 5: Professional Standards

This aspect describes how staff use of technology complies with both school and local authority policy and professional standards.

	Level	Descriptor
Aspect 5: Professional Standards	5	The school has no policies or protocols in place for the use of online communication technology between the staff and other members of the school and wider community.
	4	The school is developing policies and protocols for the use of online communication technology between the staff and other members of the school and wider community.
	3	In consultation with the staff, the school has in place policies and protocols for the use of online communication technology 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, the local authority's Acceptable Use Policy and any emerging national guidance on the responsible professional use of digital technology in education. Users know that monitoring systems are in place.
	2	In consultation with the staff, the school has in place policies and protocols for the use of online communication technology between the staff and other members of the school and wider community. Staff follow the relevant Professional Standards, the Code of Professionalism and Conduct, the local authority's Acceptable Use Policy and any emerging national guidance on the responsible professional use of digital technology in education. Members of staff understand the need for communication with children / young people, parents / carers and members of the community to take place only through official school systems (e.g. school email, Glow tools and services, learning platforms etc.) and that the communications must be professional in nature.
	1	In consultation with the staff, the school has in place policies and protocols for the use of online communication technology between the staff and other members of the school and wider community. Staff follow the relevant Professional Standards and Code of Conduct, local authority's Acceptable Use Policy and any emerging national guidance on the appropriate professional use of digital technology in education. Members of staff only use official school systems (eg. school email, Glow, learning platforms 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 online communication technology, but ensures that online safety issues have been carefully considered and policies updated before they are adopted for use.

Element B: Infrastructure

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.

Strand 1: Passwords

This strand 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 the latest local guidance/requirements?

Aspect 1: Password Security

This aspect covers the need for the school to work with their local authority to ensure the security of its systems and data through good password policy and practice. It addresses the need for age appropriate password practices and for the school to implement password records, recovery and change routines.

	Level	Descriptor
Aspect 1: Password Security	5	The school has no password policy or practices in place to protect the security of its systems and data.
	4	The school is working with the local authority to develop password policy and practices to protect the security of its systems and data. A system for managing passwords is in place, with responsibilities allocated. Appropriate staff use passwords for access to networks and devices and have received training. There are age appropriate password requirements for user access.
	3	The school has worked with the local authority and a password policy is in place to protect the security of its systems and data. There are clear management responsibilities and policy is clearly communicated, e.g. through staff handbooks and user agreements. All staff require passwords for user access to networks and devices and have received training. Routines are in place to provide appropriate access for temporary staff/users. Secure authentication is in place for staff users accessing sensitive or vulnerable data. There are age appropriate password requirements for user access and this in reinforced through the curriculum. Users should be able to recover/reset passwords.

2	The school has worked with the local authority and a password policy is in place to protect the security of its systems and data. There are clear management responsibilities and policy is clearly communicated. All users have appropriate individual password-secured access to school systems and have received education / training. Routines are in place to provide appropriate access for temporary staff/users. Secure authentication is in place for staff users accessing sensitive or vulnerable data, including access to school systems offsite. Users are able to recover / reset passwords. There are routines for regular password change which include forcing password strength at renewal. Access to systems is locked out after a set number of incorrect attempts. Incident routines are in place to resolve password compromise / violation.
1	The school has worked with the local authority and a password policy is in place to protect the security of its systems and data. There are clear management responsibilities and policy is clearly communicated. All users have appropriate individual password-secured access to school systems and have received education/training. Routines are in place to provide appropriate access for temporary staff/users. Secure authentication is in place for staff users accessing sensitive or vulnerable data, including access to school systems offsite. There are routines for regular password change which include forcing password strength at renewal. Access to systems is locked out after a set number of incorrect attempts. Incident routines are in place to resolve password compromise/violation. Dual factor or equivalent secure authentication is implemented for sensitive/ vulnerable data systems, for example MIS, external access/transfer, system administration, etc. Password related incidents are monitored and inform policy. There are regular reviews of policy and practice.

Strand 2: Services

This strand allows schools to review the security of their infrastructure and whether it meets the latest national / local guidance / requirements. 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 unauthorised access

Aspect 1: Filtering and Monitoring

This aspect covers the ability of the school to work with the local authority to manage access to content across its systems and monitor activity to safeguard users. This includes: filtering technologies; network monitoring; reporting and incident management.

	Level	Descriptor
Aspect 1: Filtering and Monitoring	5	The school provides internet access for users which is neither managed nor monitored.
	4	Internet access is filtered for all users and regularly updated. Illegal content, (e.g. child sexual abuse; extreme pornography; criminally racist or terrorist content) is filtered by actively employing illegal content lists, (e.g. IWF CAIC and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office). Filtering should also include mechanisms to protect users from accessing terrorist and extremist material and prevent people being drawn into terrorism (Counter Terrorism and Securities Act 2015). Content is managed, relevant to users' needs and inappropriate content is filtered. Internet use is logged and regularly monitored.
	3	Internet access is filtered for all users and regularly updated. Illegal content (e.g. child sexual abuse; extreme pornography or criminally racist or terrorist content) is filtered by actively employing illegal content lists (e.g. IWF CAIC list). Filtering should also include mechanisms to protect users from accessing terrorist and extremist material and prevent people being drawn into terrorism (Counter Terrorism and Securities Act 2015). Content is managed, relevant to users' needs and inappropriate content is filtered. Internet use is logged and regularly monitored.

2	Internet access is filtered for all users and regularly updated. Illegal content, (e.g. child sexual abuse; extreme pornography; criminally racist or terrorist content) is filtered by actively employing illegal content lists, (e.g. IWF CAIC and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office). Filtering should also include mechanisms to protect users from accessing terrorist and extremist material and prevent people being drawn into terrorism (Counter Terrorism and Securities Act 2015). Content is managed, relevant to users' needs and inappropriate content is filtered. Internet use is logged and regularly monitored. Differentiated internet access is available for staff and customised filtering changes are managed by the school. 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.
1	Internet access is filtered for all users and regularly updated. Illegal content (e.g. child sexual abuse; extreme pornography or criminally racist or terrorist content) is filtered by actively employing illegal content lists. (e.g. IWF CAIC and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office). Filtering should also include mechanisms to protect users from accessing terrorist and extremist material and prevent people being drawn into terrorism (Counter Terrorism and Securities Act 2015). Content is managed, relevant to users' needs and inappropriate content is filtered. Internet use is logged and regularly monitored. Differentiated internet access is available for staff and customised filtering changes are managed by the school. 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. Pro-active monitoring alerts the school to breaches of the filtering or acceptable use policy, allowing rapid response. There is an appropriate and balanced approach to providing access to online content.

Aspect 2: Technical Security

This aspect describes the ability of the school to work with the local authority to understand and ensure reasonable duty of care regarding the technical and physical security of administrative and curriculum networks (including Wi-Fi) and devices and the safety of its users.

	Level	Descriptor
Aspect 1: Policy Development	5	The school has no strategy to plan, manage or monitor the technical and physical security of its systems and devices and the safety of its users.
	4	The school is working with the local authority to develop its technical security strategy. Senior leaders understand their responsibilities regarding the provision of safe and secure technologies for all users and drive strategy development. There are clear mechanisms for network access that include user identification for all users (where age appropriate). The technical and physical security of devices and network equipment has been considered and is being implemented, including the network identification and management of devices.
	3	The school has worked with the local authority to develop a clear technical security strategy, informed by internal audit. Senior leaders are involved in and drive strategy development. Network access requires user identification for all users (where age appropriate). Devices and network equipment are physically secured and managed. Anti-virus and malware prevention is applied and regularly updated across school systems. System backups are regularly made and are an integral component of system recovery routines. The school can demonstrate an appropriate level of network resilience to external breach or attack and there are systems in place to detect and report such incidents. There are clear routines for managing security incidents that include escalation routes to appropriate authorities and external agencies.

2	The school has worked with the local authority to develop an effective technical security strategy. Senior leaders drive strategy development. Network access requires user identification for all users. Devices and network equipment are physically secured and managed. Anti-virus and malware prevention is applied and regularly updated across school systems. System backups are regularly made and are an integral component of system recovery routines. The school can demonstrate a robust level of network resilience to external breach or attack with systems in place for detection and reporting. There are clear routines for managing security incidents that include escalation routes to appropriate authorities and external agencies. The school has quality assured any external technical support or provision it uses and has assessed the impact of potential loss of service or data. There is a post incident strategy that addresses system vulnerabilities and educates / informs users.
1	The school has worked with the local authority to develop an effective technical security strategy. Senior leaders drive strategy development. Network access requires user identification for all users. Devices and network equipment are physically secured and managed. Anti-virus and malware prevention is applied and regularly updated across school systems. System backups are regularly made and are an integral component of system recovery routines. The school can demonstrate a robust level of network resilience to external breach or attack with systems in place for detection and reporting. There are clear routines for managing security incidents that include escalation routes to appropriate authorities and external agencies. The school has quality assured any external technical support or provision it uses and has assessed the impact of potential loss of service or data. There is a post-incident strategy that addresses system vulnerabilities and educates/informs users. School practice reflects up to date advancements in security, providing protection from new security threats as they arise, informed by: external review; monitoring system effectiveness; regular auditing and system testing, e.g. penetration testing. There are effective communication routes that inform the wider school community in the event of serious incidents.

Aspect 3: Data Protection

This aspect describes the ability of the school to be compliant with Data Protection and Freedom of Information legislation (including the new General Data Protection Regulations from May 2018). It describes the ability of the school to effectively control practice through the implementation of policy, procedure and education of all users.

	Level	Descriptor
Aspect 3: Data Protection	5	There are no policies ensuring compliance with legal, statutory, regulatory and contractual data requirements.
	4	The school is working with the local authority to develop a comprehensive data protection policy. Independent schools have policies meeting their requirements as data holders.
	3	The school has worked with the local authority to develop a comprehensive data protection policy. All staff know and understand their statutory obligations under current data protection law 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 has undertaken an audit to identify the personal and sensitive data it processes. Any personal data stored in the cloud has appropriate security measures in place to protect confidentiality, integrity and availability of the data. The school, in partnership with the local authority, has processes in place to manage Freedom of Information requests

2	The school has worked with the local authority to develop a comprehensive data protection policy which addresses issues such as: (but not limited to) the use of personal devices; and those devices that move between school and beyond; cloud storage; personal data; monitoring; device management and asset tracking; filtering; firewall rule; passwords and disposal. These policies are known, understood and adhered to by users. Schools understand the right of anyone to request a copy of one's own personal data through a Subject Access Request (SAR). 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 undertaken an audit to identify the personal and sensitive data it processes. Personal data is only stored in the cloud where appropriate and measures are in place to secure it which meet with statutory requirements. The organisation has appointed a data protection officer.
1	The school has worked with the local authority to develop a comprehensive data protection policy which addresses issues such as: (but not limited to) the use of personal devices; and those devices that move between school and beyond; cloud storage; personal data; monitoring; device management and asset tracking; filtering; firewall rule; passwords and disposal. The policies make provision for the school to support staff / children / young people who may access systems from beyond the school. These policies 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. The school in partnership with the local authority has systems in place to ensure that a subject access request can be met within the timescales laid out in legislation. The school has undertaken an audit to identify the personal and sensitive data it processes. Personal data is only stored in the cloud where appropriate and measures are in place to secure it which meet with statutory requirements. The organisation has appointed a data protection officer who is aware of school and local authority responsibilities and procedures. All protected data is clearly labelled. There is a clear procedure in place for audit logs to be kept and for reporting, managing and recovering from information risk incidents.

Element C: Education

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.

Strand 1: Children and Young People

This strand allows schools to review the extent to which they adequately prepare children / young people to become informed and responsible users - both within and outside school. Is online safety 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 children / young people can make to online safety in and out of school?

Aspect 1: Online Safety Education

This aspect describes how the school builds resilience in its children / young people through an effective online safety education programme.

	Level	Descriptor
Aspect 1: Online Safety Education	5	There is no planned programme of online safety education.
	4	A planned programme of online safety education is being developed, in line with Curriculum for Excellence outcomes (in particular Technologies and Health and Well Being).
	3	A planned online safety education programme takes place, either within a programme or integrated into broader Technology or Health and Wellbeing programmes. Children / young people are aware of online safety issues and can recount how to stay safe online. They understand risks and are developing confidence in protecting themselves and respecting others. A range of relevant online safety resources are used, including those that prevent people being radicalised and drawn into terrorism. Children and young people are achieving relevant outcomes within Curriculum for Excellence technologies and health and well-being.

2	A planned online 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 children / young people's progress. The curriculum should reflect the wider personal, social and technical aspects of online safety education, making use of a broad range of current and relevant resources, including those that prevent people being radicalised and drawn into terrorism. 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 online-bullying. Children and young people are developing as digital citizens.
1	A planned online 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 children / young people's progress. The curriculum reflects the wider personal, social and technical aspects of online safety education including the prevention of people being radicalised and drawn into terrorism. It 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 online safety messages in an engaged and relevant way. Children / young people are themselves involved in online safety education, e.g. through peer mentoring / education and there is evidence of differentiation for children / young people / 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 online bullying and encourage their friends to talk about difficult and negative experiences online. The school regularly evaluates the effectiveness and impact of online safety programmes.

Aspect 2: Digital Literacy

This aspect describes how the school develops the ability of children / young people to find, evaluate, use, share, and create digital content in a way that minimises risk and promotes positive outcomes.

	Level	Descriptor
Aspect 2: Digital Literacy	5	There are no opportunities for children / young people to gain an understanding of, nor practice, digital literacy skills.
	4	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; the ability to find and select information; and cultural/social understanding.
	3	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.
	2	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 / young people are aware of the opportunities that social media offers for collaboration and are beginning to operate effectively and safely within those communities.
	1	Children / 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. Children / young people use social media to collaborate and can operate effectively and safely within those communities. Digital literacy planning aligns with and complements the online safety education programme.

Aspect 3: The Contribution of Children / Young People

This aspect describes how the school maximises the potential of learner's knowledge and skills in shaping online safety strategy for the school community and how the benefits contribute to children / young people personal development.

	Level	Descriptor
The Contribution of Children / Young People	5	The school does not acknowledge nor use the skills and knowledge of children / young people in the use of new technologies in the development of its online safety strategy.
	4	The school is developing opportunities to acknowledge and use the skills and knowledge of children / young people in the use of new technologies in the development of its online safety strategy.
	3	The school acknowledges, learns from and uses the skills and knowledge of children / young people in the use of new technologies. These contribute to the development of its online safety strategy, particularly the policy and education programmes.
	2	The school acknowledges, learns from and uses the skills and knowledge of children / young people in the use of new technologies. These significantly inform school online safety policy and programmes. The school involves children / young people in delivering its online safety campaigns and in the support of peer groups. There are mechanisms to canvass feedback and opinion from children and young people. There is evidence that the involvement of children / young people contributes positively to their own personal development e.g. through peer support and digital leader programmes.
	1	The school acknowledges, learns from and uses the skills and knowledge of children / young people in the use of new technologies. These significantly inform school online safety policy and programmes. The school involves children / young people in designing and delivering its online 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. They actively contribute to parents' evenings and family learning programmes with online safety as their focus. There is evidence that children / young people involvement contributes positively to the personal development of the wider learner population, e.g. through peer support and digital leader programmes.

Strand 2: Staff

This strand allows schools/colleges to review the effectiveness of their online safety professional learning for staff. Do all (teaching and support) staff receive adequate and ongoing training and support in online safety to enable them to be safe and responsible users themselves and to be able educate and support children / young people and others in online safety?

Aspect 1: Professional Learning

This aspect describes the effectiveness of the school's online safety professional learning programme and how it prepares and empowers staff to educate and intervene in issues when they arise.

	Level	Descriptor
Professional Learning	5	There is no planned online safety training programme for staff. Child protection / safeguarding training does not include online safety.
	4	A planned online safety professional learning programme is being developed, which aligns with child protection / safeguarding training.
	3	There is a planned programme of staff online safety professional learning that is regularly revisited and updated. There is clear alignment and consistency with child protection / safeguarding training, e.g. Prevent and vice versa. Training needs are informed through audits and the induction programme for new staff includes online safety. There is evidence that key members of staff (e.g. online safety officer, Child Protection Officer, data officer) have received more specific training beyond general awareness raising. The online safety officer can demonstrate how their own professional expertise has been sustained, e.g., through conferences, research, training or membership of expert groups.

2	There is a planned programme of online safety training for all staff that is regularly revisited and updated. Staff are confident and informed in dealing with issues relating to their own personal well-being. There is clear alignment and consistency with other child protection / safeguarding training, e.g. Prevent and vice versa. Training needs are informed through audits and the induction programme for new staff includes online safety. Where relevant, online safety training is included in PRD targets. There is evidence that key members of staff (e.g. online safety officer, Child Protection Officer, data officer) have received more specific training beyond general awareness raising, some of which is accredited and recognised. The online safety officer can demonstrate how their own professional expertise has been sustained and accredited.
1	There is a planned programme of online safety professional learning for all staff that is regularly revisited and updated. Staff are confident and informed in dealing with issues relating to their own personal well-being. 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 / Prevent training and vice versa. Training needs are informed through audits and the induction programme for new staff includes online safety. Where relevant, online safety training is included in performance management targets. There is evidence that key members of staff, (e.g. online safety officer, Child Protection Officer, data officer) have received more specific training beyond general awareness raising, some of which is accredited and recognised. The online 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 online safety and that they participate more widely in local / national professional learning events. Across the school community there is a developing understanding of digital citizenship. The impact of online safety training is evaluated and informs subsequent practice.

Strand 3: Parents and Carers

This strand allows schools to review the extent to which they involve parents and carers in online safety awareness and the effectiveness of this provision. Does the school acknowledge the importance of parents and carers in online safety education and the monitoring /regulation of the children's on-line experiences (particularly out of school)? Does it provide sufficient opportunities to provide information and support to parents and carers to allow them to carry out this role?

Aspect 1: Parental Engagement

This aspect describes how the school educates and informs parents and carers on issues relating to online safety, including support for establishing effective online safety strategies for the family.

	Level	Descriptor
Aspect 4: Public Online Communications	5	The school does not provide opportunities for parents to receive information or education about online safety.
	4	The school is developing opportunities for parents to receive information or education about online safety and beginning to involve parents in discussion about these issues.
	3	The school provides some opportunities for parents to receive information or education about online safety. The school has run events / meetings for parents and carers and has referenced online safety issues in communications, (e.g. newsletter, website, social media). Parents are aware of and have acknowledged the learner acceptable use policy, where appropriate. Parents have had opportunities to share with each other and the school their attitudes to online safety and young people.
	2	The school provides regular opportunities for parents to receive information or education about online safety. There is evidence that parent online safety events / communications are effective. 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. Parents understand the links between online safety and the school's positive relations, behaviour policy and anti-bullying policies. Parents are aware of and have acknowledged the learner acceptable use agreement where appropriate and there is clear evidence of support. There is some engagement of "hard to reach" parents in online safety programmes.

1	The school provides regular opportunities for parents to receive information or education about online safety. There is evidence that parent online safety events / communications are effective. The school understands the importance of the role of parents and carers in online safety education and in the monitoring/regulation of the children's on-line experiences (particularly out of school). 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. Parents are aware of and have acknowledged the learner acceptable use agreement where appropriate, and there is clear evidence of support. Parents and carers know about the school's complaints procedure and how to use it effectively. 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. The school is effective in engaging "hard to reach" parents in online safety programmes.

Element D: Standards

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

Strand 1: Monitoring

This strand allows school/colleges to review the effectiveness of its monitoring and the impact on policy and practice. Has provision for monitoring, recording and reporting been built into the online safety policy and practice? Does the school have ways in which it can measure the effectiveness of the online 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 online safety strategy.

Aspect 1: Monitoring Online Behaviour and Responding to Incidents

This aspect covers a school's effectiveness in monitoring online behaviour and recording incidents; its response to those incidents and how they inform online safety strategy.

	Level	Descriptor
Monitoring Online Behaviour and Responding to Incidents	5	There is no system in place to monitor online behaviour and respond to incidents.
	4	A system to monitor online behaviour and record incidents is being developed. The school is developing its capacity to respond effectively when they arise.
	3	Monitoring of online behaviour takes place and records are kept, as part of normal monitoring and recording processes, (e.g. child protection / safeguarding / behaviour). Where monitoring identifies child protection / safeguarding / Prevent strategy issues, responses are appropriate and effective. The records are reviewed / audited and reported to school senior leaders and escalated to external agencies where appropriate. Parents are informed of online safety incidents, as appropriate.
	2	Detailed monitoring of online safety incidents takes place that includes (where appropriate): references to individual incidents within school and, if appropriate, incidents beyond school. Where monitoring identifies child protection / safeguarding issues, responses are appropriate and effective. Records are kept and are reviewed/audited and reported to school senior leaders and escalated to external agencies where appropriate. There are clear systems for communicating incidents with the Parent Group and with parents and carers.
	1	Detailed monitoring of online behaviour and incidents takes place that includes: references to individual incidents within school and where appropriate, incidents beyond school. Where monitoring identifies child protection / safeguarding / Prevent strategy issues, responses are appropriate and effective. Records are kept and are reviewed /audited and reported to the school senior leaders and Parent Group and escalated to external agencies where appropriate. There are clear systems for communicating incidents with parents and carers. Monitoring and reporting of incidents contributes to developments in policy and practice in online safety within the school/college. The school actively cooperates with other agencies and the Child Protection/GIRFEC groups to help ensure the development of a consistent and effective local online safety strategy. All parents and carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising.

Aspect 2: Impact of the Online Safety Policy and Practice

This aspect covers the effectiveness of a school online safety strategy; the evidence used to evaluate impact and how that shapes developments in policy and practice.

	Level	Descriptor
Impact of the Online Safety Policy and Practice	5	The impact of the online safety policy and practice is not evaluated.
	4	Systems to evaluate the impact of online safety policy and practice are being developed.
	3	The impact of the online safety policy and practice is evaluated through the review of online safety incident logs, behaviour logs, surveys of staff, children and young people, parents / carers. There is evidence that the school online safety strategy is validated or improved by these evaluations.
	2	The impact of the online safety policy and practice is evaluated through the review of online safety incident logs, behaviour logs, surveys of staff, children and young people, parents / carers. There is evidence that the school online safety strategy is validated or improved by these evaluations. The school reviews the effectiveness of online safety support received from external agencies. There is evidence of balanced professional debate about data from the logs and the impact of preventative work, e.g. online safety education, awareness and training.
	1	The impact of the online safety policy and practice is evaluated through the review of online safety incident logs, behaviour logs, surveys of staff, children and young people, parents / carers. There is evidence that the school online safety strategy is validated or improved by these evaluations. The school reviews the effectiveness of online safety support received from external agencies. There is evidence of balanced professional debate about data from the logs and the impact of preventative work, e.g. online safety education, awareness and training. The evidence of impact is shared with other school/colleges, agencies and SCB to help ensure the development of a consistent and effective local and online safety strategy. 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 online 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 online safety strategy.

Record Sheet

This record sheet should be used with the 360 degree safe online 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 1	Level 2	Level 3	Level 4	Level 5	Comment	Sources of Evidence
Strand 1	Responsibilities						
Aspect 1 Online Safety Group							
Aspect 2 Online Safety Responsibilities							

Record Sheet

Element A	Policy and Leadership						
	Level 1	Level 2	Level 3	Level 4	Level 5	Comment	Sources of Evidence
Strand 2	Policies						
Aspect 1 Policy Development							
Aspect 2 Policy Scope							
Aspect 3 Acceptable Use							

Record Sheet

Element A	Policy and Leadership						
	Level 1	Level 2	Level 3	Level 4	Level 5	Comment	Sources of Evidence
Strand 2	Policies						
Aspect 4 Self-Evaluation							
Aspect 5 Whole School							
Aspect 6 Strategies for managing unacceptable use							
Aspect 7 Reporting							

Record Sheet

Element A	Policy and Leadership						
	Level 1	Level 2	Level 3	Level 4	Level 5	Comment	Sources of Evidence
Strand 3	Communications and Communications Technologies						
Aspect 1 Mobile Technology							
Aspect 2 Social Media							
Aspect 3 Digital and Video Images							
Aspect 4 Public Online Communications							
Aspect 5 Professional Standards							

Record Sheet

Element B	Infrastructure						
	Level 5	Level 4	Level 3	Level 2	Level 1	Comment	Sources of Evidence
Strand 1	Passwords						
Aspect 1 Password Security							
Strand 2	Services						
Aspect 1 Filtering and Monitoring							
Aspect 2 Technical Security							
Aspect 3 Data Protection							

Record Sheet

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 Online Safety Education							
Aspect 2 Digital Literacy							
Aspect 3 The Contribution of Young People							

Record Sheet

Element C	Education						
	Level 5	Level 4	Level 3	Level 2	Level 1	Comment	Sources of Evidence
Strand 2	Staff						
Aspect 1 Staff Training							
Strand 3	Parent and Carers						
Aspect 1 Parental Engagement							
Strand 4	Community						
Aspect 1 Community Engagement							

Record Sheet

Element D	Standards and Inspection						
	Level 5	Level 4	Level 3	Level 2	Level 1	Comment	Sources of Evidence
Strand 1	Monitoring						
Aspect 1 Monitoring and Reporting on online safety Incidents							
Aspect 2 Impact of the Online Safety Policy and Practice							

Name of School: .....

Contact Person: .....

School Address: .....

Email Address: .....

Telephone Number: .....