School Online Safety Self-Review Tool

Updated April 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 / 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 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 model:

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.

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

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 sanctions.

Strand 1: Responsibilities

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
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 SLT, staff (including Child Protection representative), governors and pupils / students. It has clear lines of responsibility and accountability.
	1	The school has an active online safety group with wide representation from within the school e.g. SLT, teaching and support staff (including Child Protection representative), governors and pupils / students and also from parents and carers and the wider community. It has clear lines of responsibility and accountability which are understood by all members of the school. The committee is actively integrated and collaborating with other relevant groups in school.

Aspect 2: Online Safety Responsibilities

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

	Level	Descriptor
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 a designated Online Safety Coordinator / Officer with clear responsibilities.
	2	The school has a designated Online Safety Coordinator / Officer with clear responsibilities. These include leadership of the Online Safety group, staff training and awareness. Designated persons are responsible for monitoring incidents and handling sensitive issues (including child protection). Many staff take responsibility for online safety.
	1	The school has a designated Online Safety Coordinator / Officer 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. Designated persons are responsible for monitoring incidents and handling sensitive issues. All staff take active responsibility for online safety.

Aspect 3: Governors

This aspect describes Governors' (or those in a similar position e.g. a Board of Directors) online safety accountabilities and how the school ensures this influences policy and practice.

	Level	Descriptor
Governors	5	The Governors are not involved in online safety policy and provision.
	4	The Governors are aware that the school is developing aspects of its online safety policy and provision, but they are not involved in the development
	3	Governors understand their online safety responsibilities and accountabilities. There is evidence of online safety knowledge on the Governing Body. They are involved in the development of the online safety policy and approve it. Governors receive online safety reports from senior leaders.
	2	Governors understand their online safety responsibilities and accountabilities. There is evidence of online safety knowledge on the Governing Body. They are involved in the development of the online safety policy and approve it. Governors receive and act upon online safety reports from senior leaders. A Governor is part of the Online Safety Group and is able to provide support and critically challenge to the school on policy and practice. Governors allocate resources to provide online safety education.
	1	Governors understand their online safety responsibilities and accountabilities. There is evidence of online safety knowledge on the Governing Body. They are involved in the development of the online safety policy and approve it. Governors receive and act upon online safety reports from senior leaders. A Governor is part of the Online Safety Group and is able to provide challenge to the school on policy and practice. Governors allocate resources to provide online safety education and are given the opportunity to regularly update their knowledge. Governors receive regular monitoring reports on the implementation of the online safety policy. Governors are involved in the promotion of online safety in the wider community

Strand 2: Policies

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 safeguarding obligations. It has been developed in consultation with a wide range of staff and pupils / students. 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 safeguarding obligations. It has been developed in consultation with the staff, pupils / students, parents and the wider community. There is widespread ownership of the policy. The policy is reviewed annually and more frequently in light of changes in technology or 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 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 roles and 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. The policy clearly states the school's commitment to act on online safety incidents outside the school that affect the well-being of staff and pupils / students
	1	The online 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 roles and issues such as social networking, online bullying, data protection, passwords, filtering, digital and video images and use of mobile and / or gaming devices. It establishes school expectations regarding ethics and behaviour of all users. The policy clearly states the school's commitment to act on online safety incidents outside the school that affect the wellbeing of staff and pupils / students. 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 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	Guidance for users on the acceptable use of technology is being developed
	3	Guidance on the acceptable use of technology is provided for all users of technology on the school site.
	2	Guidance on the acceptable use of technology is provided for all users of technology on the school site. These expectations are clearly and regularly communicated. The guidance is aligned with relevant existing policies and embedded within the culture of the school. Where Acceptable Use Agreements are used, these may be acknowledged by pupils / students 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 young people and adults who are new to the school are informed of expectations of acceptable use.
	1	Guidance on the acceptable use of technology is provided for all users of technology on the school site. These expectations are clearly and regularly communicated. The guidance is aligned with relevant existing policies and embedded within the culture of the school. Where Acceptable Use Agreements are used, these may be acknowledged by pupils / students 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 young people and adults who are new to the school are 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 the school's wider self-evaluation processes e.g. team self-reviews, LA reviews, NAACE Self Review Framework.
	4	The school has begun to consider online safety within the school's wider self-evaluation processes e.g. team self-reviews, LA reviews, NAACE Self Review Framework.
	3	The school's wider self-evaluation processes address online safety. There is reference to online safety in documents such as team self-reviews, LA reviews, NAACE Self Review Framework. The school has identified and acknowledged some areas of strength and weakness and priorities for action.
	2	Online safety is a strong feature within the school's wider self-evaluation processes. Documents such as team self-reviews, LA reviews, NAACE Self Review Framework clearly acknowledges areas of strength and weakness and priorities for action. The school has made use of pupil / student and parent / carer surveys in identification of strengths, weaknesses and priorities. The school may be using the NAACE Self Review Framework in preparation for an ICT Mark submission or the SWGfL 360Data Protect self-review tool for data protection and information security.
	1	Online safety is a strong feature within the school's wider self-evaluation processes. Documents such as team self-reviews, LA reviews, ICT Self Review Framework clearly acknowledge areas of strength and weakness and priorities for action. The school has made use of pupil / student, parent / carer and community user surveys in identification of strengths, weaknesses and priorities. The school has achieved or is in the process of achieving ICT Mark (or similar recognised quality marks).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 / safeguarding practices and vice versa e.g. behaviour, anti-bullying, Prevent Action Plan; PHSE, 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	The school is beginning to link online safety into other whole school policies / strategies
	3	Online safety is referred to in other whole school policies / strategies e.g. behaviour, anti-bullying, Prevent Action Plan, PHSE, Child Protection / Safeguarding and computing.
	2	There are clear and consistent links between the school online safety policy and sections of other policies / strategies where there is reference to online safety e.g. in the behaviour, anti-bullying, Prevent Action Plan, PHSE, Child Protection / Safeguarding and computing policies.
	1	Online safety is embedded in all relevant whole school policies / 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, 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 / strategies as the behaviour, anti-bullying, Prevent Action Plan; PHSE, Child Protection/ Safeguarding and computing policies.

Aspect 6: Strategies for Managing Unacceptable Use

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

	Level	Descriptor
Aspect 6: Strategies for Managing Unacceptable Use	5	There are no strategies for managing unacceptable use.
	4	There are strategies for managing unacceptable use but these are not linked to agreed policy on acceptable use and are not consistently enforced.
	3	Strategies for managing unacceptable 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 managing unacceptable use are clearly stated in the online safety policy and relevant school policies and users are aware of these strategies. Staff and student / pupil consultation has been part of the decision making process. The school acknowledges and celebrates positive use. Users understand that the school may take action and intervene, where appropriate, in online incidents that take place beyond school. Strategies are regularly reviewed in the light of current practice and changes in technology.
	1	Strategies for managing unacceptable use are clearly stated in relevant school policies and users are aware of these strategies. Staff and student / pupil consultation has been part of the decision making process. The school celebrates and rewards positive use. Users understand that the school may take action and intervene, where appropriate, in online incidents that take place beyond school. Strategies are regularly reviewed in the light of current practice and changes in technology. The school is rigorous in monitoring and applying an appropriate and differentiated range of strategies. There is a clear and positive behavioural online culture and interventions are rare

Aspect 7: Reporting

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

	Level	Descriptor
Aspect 7: Reporting	5	Users are unclear about their responsibilities to report online safety incidents and there is no clear process for reporting 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 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 CEOP.
	2	Users understand their responsibilities to report online 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. There are clear escalation processes for the handling of 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 (e.g. local authority and regional broadband grid) in dealing with online safety issues. Reports are logged for future auditing / monitoring. Users have an understanding of how to report issues online, including to CEOP.
	1	There are clearly known and understood systems for reporting online 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 (e.g. the local authority and regional broadband grid) in dealing with online safety issues. There are good links with outside agencies e.g. 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

Aspect 1: Mobile Technology

This aspect considers the benefits and challenges of mobile technologies; their use in a school environment and beyond; the effective management of 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. "BYOD".

	Level	Descriptor
Aspect 1: Policy Development	5	There is no policy relating to the use of mobile technology
	4	A policy relating to the use of mobile technology is being developed and is in the process of being implemented.
	3	The school has a policy relating to the use of mobile technology that covers staff, visitors and pupil / student use and, where applicable, the use of mobile technology provided by the school.
	2	The school has a clearly understood and accepted policy relating to the use of mobile technology that covers staff, visitors and pupil / student use and, where applicable, the use of mobile technology provided by the school. 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 should be clear guidance.
	1	The school has a clearly understood and accepted policy relating to the use of mobile technology that covers staff, visitors and pupil / student use and, where applicable, the use of mobile technology provided by the school. 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. The school has realised the educational potential of these devices and has encouraged and implemented their safe use within school to support teaching and learning. 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 is being developed which includes statements about a planned programme of education.
	3	The school has 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. The school is aware of the impact of social media comments made about it by others.
	2	The school has clearly understood and accepted policies relating to the use, by staff, students / pupils and other school users of social media. The policy clearly references a planned programme of education. 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 (if allowed) and beyond. The school understands the impact of social media comments about both the school and its community and has begun to implement appropriate responses where necessary.
	1	The school has clearly understood and accepted policies relating to the use of social media. The policy clearly references a planned programme of education. 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 (if allowed) and beyond. The school has realised the educational potential of social media and has developed the use of social media technologies within the curriculum e.g. blogging, where this is relevant and age appropriate to learning. 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.

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 the Data Protection Act.

	Level	Descriptor
Aspect 1: Policy Development	5	There is no policy relating to the use and publication of digital and video images.
	4	A policy relating to the use and publication of digital and video images is being developed.
	3	The school has policies relating to the use and publication of digital and video images and parental permission is sought, as required. The policies also reference the use of digital images by pupils / students as part of their learning.
	2	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.
	1	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 promote the quality of their teaching and learning, but are also educated about the risks.

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, online newsletters etc.
	4	There are limited references to online safety on the school's website, learning platform, 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. The school 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 school calendars and personal information – ensuring that there is no 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. The school 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 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 online safety of members of the wider community. 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 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. Staff follow the relevant Professional Standards and other national guidance. 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 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 (e.g. school email, technology platform 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 other national guidance about these technologies. Members of staff only use official school systems (e.g. school email, technology 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

Aspect 1: Password Security

This aspect covers the ability of the school 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 developing a 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 pupil / student user access.
	3	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. Secure authentication is in place for staff users accessing sensitive or vulnerable data. There are age appropriate password requirements for pupil / student user access and this in reinforced through the curriculum. Users are able to recover / reset passwords.

	2	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. 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	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. 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 e.g. 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

Aspect 1: Filtering and Monitoring

This aspect describes how the online safety policy is consistent with school expectations in other relevant policies / safeguarding practices and vice versa e.g. behaviour, anti-bullying, Prevent Action Plan; PHSE, Child Protection / Safeguarding and computing policies. There is evidence that the policy is embedded across the school.

	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, but the filtering is neither regularly monitored nor 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).
	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 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. 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 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. 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 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 developing 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 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. Antivirus & 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 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 & 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 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 & 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 the current Data Protection Act and Freedom of Information legislation (which includes the General Data Protection Regulation compliance). It describes the ability of the school to effectively control practice through the implementation of policy, procedure and education of all users. To reflect the changes that schools are required to make under the new legislation, the benchmark level for this aspect will be increased to level 2 in early 2019.

	Level	Descriptor
Aspect 3: Data Protection	5	There are no policies ensuring compliance with legal, statutory, regulatory and contractual data requirements. The school has not yet paid the relevant fee to the Information Commissioner's Office (ICO).
	4	The school is developing a comprehensive Data Protection Policies. The school has paid the relevant fee to the Information Commissioner's Office (ICO). Data subjects are informed about their rights and about the use of personal data (e.g. through a Privacy Notice).
	3	The school has a comprehensive set of Data Protection Policies. Data subjects are informed about their rights and about the use of personal data (e.g. through a Privacy Notice). The school has appointed a Data Protection Officer (DPO) who actively monitors compliance with the law and provides independent appropriate advice to senior leaders. The DPO has led a data audit / mapping exercise to understand where data currently resides, including third parties and cloud storage. The Governors/Directors responsibilities for the development and approval of Data Protection policy and procedure are clearly defined. The school has identified the personal data which it has a legal basis to process and has obtained consent for any additional data processing activity. The school has processes in place to manage Freedom of Information requests. There are procedures for the recording of subject access request and data breaches have been developed. Through training, staff are aware of their data protection responsibilities.

2	The school has a comprehensive set of Data Protection Policies the content of which includes; purpose, privacy notices and consent, Freedom of Information (FOI) and publication scheme, roles and responsibilities, training and awareness, Data Protection Impact Assessments (DPIA), audit logging, special categories of data, secure storage and access to data, subject access requests, secure transfer of data and access outside school, disposal, incident handling). The school has appointed data managers or controllers to support the Data Protection Officer (where relevant). The school has undertaken a data audit / mapping exercise to understand where data currently resides, including third parties and cloud storage. All staff know and understand their statutory obligations under the current Data Protection Act. Data subjects are informed about their rights and about the use of personal data (e.g. through a Privacy Notice). The school has effective processes in place to manage Freedom of Information requests. The recording of subject access requests and data breaches is implemented. The Governors/Directors accept responsibility for the development and approval of Data Protection Policy and procedure. Resources are allocated to Data Protection. The school has identified the personal data which it has a legal basis to process and has obtained consent for any additional data processing activity. The school has data retention policy and processes in place, safely disposing of data as defined. Data protection is enhanced through the use of encryption/two factor authentication for the handling or transfer of sensitive data.
1	The school has a comprehensive set of Data Protection Policies the content of which includes; purpose, privacy notices and consent, Freedom of Information (FOI) and publication scheme, roles and responsibilities, training and awareness, Data Protection Impact Assessments (DPIA), audit logging, special categories of data, secure storage and access to data, subject access requests, secure transfer of data and access outside school, disposal, incident handling). The school has undertaken a data audit / mapping exercise to understand where data currently resides, including third parties and cloud storage. All staff know and understand their statutory obligations under the current Data Protection Act. Data subjects are informed about their rights and about the use of personal data (e.g. through a Privacy Notice). The school has effective processes in place to manage Freedom of Information requests. The recording of subject access requests and data breaches is implemented. Governors/Directors accept responsibility for the development, approval and review of Data Protection Policy and procedure. Resources are allocated to Data Protection, which is standing agenda item at relevant meetings. The school has identified the personal data which it has a legal basis to process and has obtained consent for any additional data processing activity. The school has appointed a Data Protection Officer supported by data managers or controllers (where relevant). Data protection

is enhanced through the use of encryption/two factor authentication for the handling or transfer of sensitive data. All special categories of data are clearly identified. There is an effective procedure in place for maintaining audit logs and for reporting, managing and recovering from information risk incidents. The recording of subject access requests and data breaches is exemplary and informs changes to practice. The school actively ensures that there is 'data protection by design' when starting any new processing activity.

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

Aspect 1: Online Safety Education

This aspect describes how the school builds resilience in its pupils / students 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.
	3	A planned online safety education programme takes place. Pupils / students are aware of online safety issues and can recount how to stay safe online. A range of relevant online safety resources are used, including those that prevent people being radicalised and drawn into terrorism.
	2	A planned online safety education programme takes place through both discrete lessons and wider curriculum opportunities. The entitlement of pupils / students 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 pupil / student 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.

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 pupils / students 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 pupil / student 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. Young people are themselves involved in online safety education e.g. through peer mentoring and there is evidence of differentiation for learners / vulnerable groups. 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 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 pupils / students to gain an understanding of, nor practice, digital literacy skills.
	4	Opportunities for pupils / students 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.
	3	Pupils / students 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.
	2	There are opportunities in a wide range of lessons for pupils / students to be taught to be critically aware of the content they access on-line and how to validate the accuracy of information. Pupils / students 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. Pupils / students are aware of the opportunities that social media offers for collaboration and are beginning to operate effectively and positively within those communities.
	1	Pupils / students 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. Pupils / students 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. Pupils / students 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 Young People

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

	Level	Descriptor
Aspect 3: The Contribution of Young People	5	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 online safety strategy.
	4	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 online safety strategy
	3	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 online safety strategy, particularly the policy and education programmes.
	2	The school acknowledges, learns from and uses the skills and knowledge of young people in the use of new technologies. These significantly inform school online safety policy and programmes. The school involves pupils / students in delivering its online safety campaigns and in the support of peer groups. There are mechanisms to canvass pupil / student feedback and opinion. There is evidence that young peoples' involvement 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 young people in the use of new technologies. These significantly inform school online safety policy and programmes. The school involves pupils / students 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 pupil / student feedback and opinion. Young people actively contribute to parents' evenings and family learning programmes with online safety as their focus. There is evidence that young peoples' involvement contributes positively to the personal development of the wider pupil / student population eg through peer support and digital leader programmes.

Strand 2: Staff

Aspect 1: Staff Training

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

	Level	Descriptor
Aspect 1: Policy Development	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 staff training programme is being developed, which aligns with Child Protection and Safeguarding training
	3	There is a planned programme of staff online safety training that is regularly revisited and updated. There is clear alignment and consistency with other Child Protection / Safeguarding training 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 wellbeing. 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 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.

1	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. 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 / 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 Performance Management targets. There is evidence that key members of staff (eg 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. The impact of online safety training is evaluated and informs subsequent practice.

Strand 3: Governors

Aspect 1: Governor Education

This aspect describes the school's provision for the online safety education of Governors to support them in the execution of their role.

	Level	Descriptor
Aspect 1: Governor Education	5	There is no opportunity for Governors to receive online safety education.
	4	Opportunities for Governor online safety education are being explored.
	3	The school has identified or provided online safety education opportunities for Governors and at least one Governor has attended. There is evidence of impact.
	2	The school has identified or provided online safety education opportunities for Governors and more than one Governor has attended. There is evidence that the Governor education impacts on how the school shapes policy and practice.
	1	The school has ensured that Governors have accessed a wide range of online safety education opportunities, resulting in the ability of Governors to rigorously and strategically challenge how the school shapes policy and practice The Online Safety Group Governor has received additional focussed online safety input in response to new developments and issues associated with technology, to further inform their role.

Strand 4: Parents and Carers

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.
	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 Pupil / Student Acceptable Use Agreement, where appropriate.
	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 are aware of and have acknowledged the Pupil / Student Acceptable Use Agreement where appropriate, and there is clear evidence of support.
	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 Pupil / Student 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 is effective in engaging "hard to reach" parents in online safety programmes.

Strand 5: Community

Aspect 1: Community Engagement

This aspect describes how the school communicates and shares best practice with the wider community including local people, agencies and organisations.

	Level	Descriptor
Aspect 1: Community Engagement	5	The school does not communicate and share best practice with the wider community
	4	The school is developing opportunities to communicate and share best practice with the wider community.
	3	The school provides opportunities to communicate and share best practice with the wider community. In its engagement with other agencies opportunities are developed to draw on a wider body of expertise and perspective that enhances its own online safety provision e.g. joint projects with other schools / organisations / Prevent partner agencies / LSCBs, transition activities, external speakers etc. Safer Internet Day acts as a focus for some of these activities
	2	The school provides opportunities to communicate and share best practice with the wider community. In its engagement with other agencies opportunities are developed to draw on a wider body of expertise and perspective that enhances its own online safety provision e.g. joint projects with other schools / organisations / Prevent partner agencies / LSCBs, transition activities, external speakers etc. Safer Internet Day acts as a focus for some of these activities. There is evidence of planned online safety activities e.g. family learning courses, cross-generational learning etc. Plans are in place to increase community involvement with other local groups e.g. early years settings, youth groups, voluntary groups, libraries, police, health and support their development through the use of online safety planning tools e.g. Online Compass.

1

The school provides opportunities to communicate and share best practice with the wider community. In its engagement with other agencies opportunities are developed to draw on a wider body of expertise and perspective that enhances its own online safety provision e.g. joint projects with other schools / organisations / Prevent partner agencies / LSCBs, transition activities, external speakers etc. Safer Internet Day acts as a focus for some of these activities.

The school recognises the significant role that the local community can play in improving the quality of education and levels of aspiration. The culture of the school ensures that members of the local community are involved, whenever possible, in the planning of community programmes and in the delivery of programmes in school.

The school works with community groups and other schools / agencies e.g. early years settings, youth groups, voluntary groups, libraries, police, health etc. and supports their development through the use of online safety planning tools e.g. Online Compass. Where relevant these organisations are encouraged to apply for Online Compass Awards.

Element D: Standards and Inspection

Strand 1: Monitoring

Aspect 1: Monitoring and Reporting on Online Safety Incidents

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

	Level	Descriptor
Aspect 1: Monitoring and Reporting on Online Safety Incidents	5	There is no monitoring of online safety incidents.
	4	A process for the monitoring of online safety incidents is being developed.
	3	Monitoring of online safety incidents takes place and records are kept, as part of the school's normal monitoring and recording processes (e.g. child protection / behaviour). Where monitoring identifies safeguarding issues, interventions are appropriate and effective. The records are reviewed / audited and reported to the school's senior leaders and escalated to external agencies where appropriate. Parents are informed of online safety incidents, as relevant.
	2	Detailed monitoring of online safety incidents takes place that includes: references to individual incidents within school; incidents beyond school and regular technical reports from system monitoring. Where monitoring identifies safeguarding issues, interventions are appropriate and effective. Discrete records are kept and are reviewed / audited and reported to the school's senior leaders and Governors and escalated to external agencies where appropriate. There are clear systems for communicating incidents with parents.
	1	Detailed monitoring of online safety incidents takes place that includes: references to individual incidents within school; incidents beyond school and regular technical reports from system monitoring. Where monitoring identifies safeguarding issues, interventions are appropriate and effective. Discrete records are kept and are reviewed / audited and reported to the school's senior leaders and Governors and escalated to external agencies where appropriate. There are clear systems for communicating incidents with parents. Monitoring and reporting of incidents contributes to developments in policy and practice in online safety within the school. The school actively cooperates with other agencies and the LSCB to help ensure the development of a consistent and effective local online safety strategy. All parents / 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's online safety strategy; the evidence used to evaluate impact and how that shapes developments in policy and practice.

	Level	Descriptor
Aspect 2: 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, students / pupils, 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, students / pupils, 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 balanced professional debate about the evidence taken 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, students / pupils, 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 balanced professional debate about the evidence taken 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 schools, agencies and LSCB 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							
Aspect 3 Governors							

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

Record Sheet

Element D	Standards and Inspection						
	Level 1	Level 2	Level 3	Level 4	Level 5	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: .....