



School E-Safety Self Review Tool

Updated February 2010

School E-Safety Self Review Tool



Contents

- 1 Introduction
- 2 How to use the Self Review Tool
- 3 Links to documents and resources
- 4 Acknowledgements
- 5 Self Review Tool
- 6 Report Sheet

Introduction

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT skills, not only to 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 ICT can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks." However, schools must, through their e-safety policy and

practice, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher and governors to the senior leaders and classroom teachers, support staff,

parents, members of the community and the students / pupils themselves.

The Self Review Tool is intended to help schools to review their current e-safety policy and practice and provide:

- Management information and stimulus that can influence the production or review of e-safety policies and develop good practice
- A process for identifying strengths and weaknesses
- Opportunities for commitment and involvement from the whole school
- A continuum for schools to discuss how they might move from a basic level provision for e-safety to practice that is aspirational and innovative.

The Self Review Tool is now available as an online tool, providing a more interactive and comprehensive method to review E-Safety in schools. Further details of the online tool and the accompanying E-Safety Mark can be found at: www.360safe.org.uk



School E-Safety Self Review Tool

How to use the Self Review Tool

The self review tool enables you to review your school's current practice over four main elements, based on the Becta 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

There is little or nothing in place.

LEVEL 4

Policy and practice is being developed

LEVEL 3

Basic e-safety policy and practice is in place

LEVEL 2

Policy and practice is coherent and embedded

LEVEL 1

Policy and practice is aspirational and innovative

For each aspect, the benchmark level for the E-Safety Mark is shown in red ink.

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

The record sheet also includes sections for comments – which schools may wish to use to clarify their choice of level or as an aide-memoire to further actions. The sources of evidence column may help schools to share knowledge and information among those involved in the review. It may also be helpful to any external consultant or adviser that the school might wish to involve in its audit, review or policy development.

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



School E-Safety Self Review Tool

Links to documents and resources

South West Grid for Learning: (SWGfL Safe) - <http://www.swgfl.org.uk/safety/default.asp>

The site contains a wide range of policy documents, resources and links to other sites. Of particular interest to schools will be the "School E-Safety Policy Template".

Byron Review ("Safer Children in a Digital World") <http://www.dcsf.gov.uk/byronreview/>

Becta

Website e-safety section - <http://schools.becta.org.uk/index.php?section=is>

Developing whole school policies to support effective practice: <http://publications.becta.org.uk/display.cfm?resID=25934&page=1835>

"Safeguarding Children in a Digital World" http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_tl_rs_03&rid=13344

Data Protection: - http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_saf_dp_03

Information Management Strategy - http://schools.becta.org.uk/index.php?section=lv&&catcode=ss_lv_saf_dp_03&rid=16037

Information Commissioners Office - Data Protection: http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx

Acknowledgements

SWGfL would like to acknowledge:

- The SWGfL E-Safety Group who have been responsible for the production of this Self Review Tool.
- Becta – whose policy documents and self review frameworks have been used for reference in the production of this self review tool. .
- NEN – for reference to their E-Safety Audit Tool
- WMNet – for reference to their WMNet E-Safety Framework

Copyright of this Self Review Tool is held by SWGfL. LSCBs and member agencies are permitted free use of the tool for the purposes of their own self review. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

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

School E-Safety Self Review Tool

Element 1 of 4

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

Element A Policy and Leadership - Strand 1 - Responsibilities

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

South West Grid For Learning E-safety Self Review Tool (E-Safety Mark benchmark levels are shown in red)

ELEMENT A

Policy & Leadership

STRAND 1

Responsibilities

	Level 5	Level 4	Level 3	Level 2	Level 1
Aspect 1 E-Safety Committee	There is no e-safety committee.	The school is in the process of establishing an e-safety committee.	The school has an e-safety committee with staff representation and a clear brief.	The school has an active e-safety committee with wide representation from the SLT, staff (including child protection representative), governors and pupils / students. It has clear lines of responsibility and accountability.	The school has an active e-safety committee with wide representation from within the school eg 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 E-safety responsibilities	No one has responsibility for e-safety across the school.	One or more members of staff have responsibility for e-safety, but there is little coordination of their work.	The school has a designated E-Safety Coordinator / Officer with clear responsibilities, as in Becta guidance.	The school has a designated E-Safety Coordinator / Officer with clear responsibilities, as in Becta guidance. These include leadership of the e-safety committee, staff training and awareness. A small group is responsible for monitoring and dealing with sensitive issues (including Child Protection) Many staff take responsibility for e-safety.	The school has a designated E-Safety Coordinator / Officer with clear responsibilities, as in Becta guidance. These include leadership of the e-safety committee, staff training and awareness, commitment to and coordination of an e-safety programme with the wider community. A small group is responsible for monitoring and dealing with sensitive issues. All staff take active responsibility for e-safety.
Aspect 3 Governors	There is no Governor involvement in e-safety.	The Governors are aware that an e-safety policy is being developed, but they are not involved in its development.	Governors are aware that an e-safety policy is being developed. There is some Governor involvement in the development and approval of the e-safety policy.	Governors are involved in the development and approval of the e-safety policy. There is an appointed E-Safety Governor who is a member of the e-safety committee. Governors are aware of their responsibilities with regard to e-safety. Governors allocate resources to provide e-safety education.	Governors are involved in the development and approval of the e-safety policy. There is an appointed E-Safety Governor. All Governors are aware of their responsibilities with regard to e-safety. Governors receive regular monitoring reports on the implementation of the e-safety policy and on reported incidents. Governors are involved in the promotion of e-safety in the wider community.

What evidence could you use?

School vision and aims

School Improvement Plan

Self Evaluation documents

Job descriptions

Minutes of meetings of relevant groups, and committees, including Governors

Incident logs and monitoring reports

Moving forward – the school might wish to consider: How to engage all stakeholders, including staff, young people, parents and carers, Governors and members of the community in the establishment of the e-safety policy and their involvement in the e-safety committee and other relevant groups. Do all stakeholders know, understand and accept their responsibilities?

Element 1 of 4

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

Element A Policy and Leadership - Strand 2 - Policies (aspects 1 to 3)

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

ELEMENT A
Policy & Leadership
STRAND 2
Policies

	Level 5	Level 4	Level 3	Level 2	Level 1
Aspect 1 Policy development	There is no e-safety policy.	The school is in the process of establishing an e-safety policy.	The school has an e-safety policy, which is aligned with national, regional and LA policies.	The school has an e-safety policy, which is aligned with national, regional and LA policies and 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 annually.	The school has an e-safety policy which is aligned with national, regional and LA policies and 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 e-safety incidents. The policy is an integral part of School Improvement Planning.
Aspect 2 Policy scope	There is no e-safety policy.	The school is in the process of establishing an e-safety policy.	The e-safety policy is limited to the use of the ICT systems, equipment and software in school.	The e-safety policy covers the use of the ICT systems, equipment and software in school and also addresses issues related to the use of school related ICT out of school and the use of personal ICT equipment in school. It is comprehensive in that it includes sections on issues such as cyber-bullying, data protection, passwords, filtering, digital and video images and use of mobile / hand held devices.	The e-safety policy covers the use of the ICT systems, equipment and software in school and also addresses issues related to the use of school related ICT out of school and the use of personal ICT equipment in school. It is comprehensive in that it includes sections on issues such as cyber-bullying, data protection, passwords, filtering, digital and video images and use of mobile / hand held devices. The policy clearly states the school's responsibility and commitment to take action over school related e-safety incidents that take place out of school. The e-safety policy is differentiated and age related, in that it recognises the needs of young people at different ages and stages within the school.
Aspect 3 Acceptable Use Policies	There are no Acceptable Use Policies.	Acceptable Use Policies are being developed.	Acceptable Use Policies are in place for pupils / students and staff.	Acceptable Use Policies are in place for, and are signed by pupils / students and staff / adult volunteers. Parents receive and countersign copies of the Pupil / Student AUP. There are clear induction policies to ensure that young people and adults who are new to the school are informed of and required to sign AUPs.	Acceptable Use Policies, which are differentiated by age and stage, are in place for, and are signed (annually) by, pupils / students, staff /adult volunteers and community users. Parents receive and, annually, countersign copies of the Pupil / Student AUP. There are clear induction policies to ensure that young people and adults who are new to the school are informed of and required to sign AUPs. All users have knowledge of the e-safety policy and AUP and understand their responsibilities, as described in the policy.

What evidence could you use?

E-Safety Policy

School Development Plan

Minutes of the E-Safety Committee / other groups

Information for parents – letters, AUP, newsletter, website etc

Home-school agreements

Acceptable Use Policies (signed)

Induction policies and procedures

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

Element 1 of 4

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

Element A Policy and Leadership - Strand 2 - Policies (aspects 4 and 5)

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

ELEMENT A
Policy & Leadership
STRAND 2
Policies

	Level 5	Level 4	Level 3	Level 2	Level 1
Aspect 4 Self Evaluation	E-Safety is not considered within the school's wider self evaluation processes eg Ofsted SEF, team self reviews, LA reviews, Becta SRF.	The school has begun to consider e-safety within the school's wider self evaluation processes eg Ofsted SEF, team self reviews, LA reviews, Becta SRF.	The school's wider self evaluation processes address e-safety. There is reference to e-safety in documents such as the Ofsted SEF, team self reviews, LA reviews and Becta ICT SRF. The school has identified and acknowledged some areas of strength and weakness and priorities for action.	E-safety is a strong feature within the school's wider self evaluation processes. Documents such as the Ofsted SEF, team self reviews, LA reviews and Becta SRF clearly acknowledge 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 is using the Becta ICT SRF or similar tool and may be considering an ICT Mark submission or similar quality assurance mark.	E-safety is a strong feature within the school's wider self evaluation processes. Documents such as the Ofsted SEF, team self reviews, LA reviews and Becta SRF 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 quality assurance mark. The school openly celebrates its e-safety successes in its wider self evaluation processes.
Aspect 5 Whole School	E-safety is not referred to in other whole school policies.	The school is beginning to link e-safety into other whole school policies.	E-Safety is referred to in other whole school policies eg behaviour, anti-bullying, PHSE, Child Protection / Safeguarding and ICT.	There are clear and consistent links between the school e-safety policy and sections of other policies where there is reference to e-safety eg in the behaviour, anti-bullying, PHSE, Child Protection / Safeguarding and ICT policies.	E-safety is embedded in all relevant whole school policies. The school has carefully considered its approach to e-safety and provides a consistent e-safety message to all members of the school community, through a variety of media and activities. That promote whole school input. This is particularly apparent in the references to e-safety within such policies as the behaviour, anti-bullying, PHSE, Child Protection/ Safeguarding and ICT policies.

- What evidence could you use?**
- SEF
 - Ofsted Report
 - LA and other external reviews
 - Team and department self evaluation
 - Surveys
 - Whole school policies eg anti-bullying, PHSE, Child Protection / Safeguarding and ICT.

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

Element 1 of 4

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

Element A Policy and Leadership - Strand 2 - Policies (aspects 6 and 7)

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

ELEMENT A
Policy & Leadership
STRAND 2
Policies

	Level 5	Level 4	Level 3	Level 2	Level 1
Aspect 6 Sanctions	There are no sanctions for e-safety abuse or misuse.	There are sanctions for e-safety abuse or misuse, but these are not linked to an agreed policy / AUP and are not consistently enforced.	Sanctions for e-safety abuse or misuse are clearly stated in the e-safety policy. Users are aware of these sanctions.	Sanctions for e-safety abuse or misuse are clearly stated in the e-safety policy. Users understand the importance of sanctions and generally adhere to the e-safety policy.. A positive rewards policy balances the sanctions policy. Users understand that sanctions can be applied to e-safety incidents that take place out of school, if they are related to school (eg cyber bullying).	Sanctions for e-safety abuse or misuse are clearly stated in the e-safety policy. Users understand the importance of the sanctions and few users fail to adhere to the e-safety policy. A positive rewards policy balances the sanctions policy. Users understand that sanctions can be applied to e-safety incidents that take place out of school, if they are related to school (eg cyber bullying). The school is strict in monitoring and applying the e-safety policy and a differentiated and appropriate range of sanctions,, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions.
Aspect 7 Reporting	Users are unclear about their responsibilities to report e-safety incidents and there is no clear process for reporting abuse.	Systems (including supervision, where appropriate) and processes are in place for users to report e-safety incidents and abuse. These are not yet consistently understood or consistently used.	Users understand their responsibilities to report e-safety incidents. They know and understand that there is a clear system 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 understand their responsibilities to report e-safety incidents. They know, understand and use a clear system for reporting abuse and understand that processes must be followed rigorously. 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 e-safety incidents. The school actively seeks support from the local authority and regional broadband grid in dealing with e-safety issues.	There are clearly known and understood systems for reporting e-safety incidents. The culture of the school encourages all members of the school and its wider community to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes. Reports are logged and regularly audited and monitored. The school actively seeks support from the local authority and regional broadband grid in dealing with e-safety issues. There are good links with outside agencies eg the police who can help the school and members of the community in dealing with these issues. The school contributes to consistent monitoring / reporting practice across the local area through the LSCB e-safety group, or similar.

What evidence could you use?

Behaviour and anti-bullying policies

Rewards and sanctions policies

Posters in classrooms / on-screen messages

AUPs

Incident logs with evidence of monitoring and auditing.

Communications with external agencies

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

School E-Safety Self Review Tool

Element 1 of 4

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

Element A Policy and Leadership - Strand 3 - Communications and Communications Technologies (aspects 1 and 2)

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

ELEMENT A

Policy & Leadership

STRAND 3

Communications and Communications Technologies

	Level 5	Level 4	Level 3	Level 2	Level 1
Aspect 1 Mobile phones and personal hand held devices	There is no policy relating to the use of mobile phones and personal hand held devices by young people and adults.	A policy relating to the use, by young people and adults, of mobile phones and personal hand held devices is being developed.	The school has a policy relating to the use of mobile phones and personal hand held devices by young people and adults.	The school has clearly understood and accepted policies relating to the use of mobile phones and personal hand held devices, by young people and adults. Users understand the risks associated with the use of these devices and are encouraged to be responsible users, both inside school (if allowed) and outside school. The school realises the educational potential of these devices and is investigating how they might be used safely in school.	The school has clearly understood and accepted policies relating to the use of mobile phones / hand held devices, by young people and adults. Users have a mature approach to their safe use. The school has realised the educational potential of these devices and has allowed / encouraged their safe use within school, where this is relevant to the learning that is taking place. There are clear and enforced sanctions for misuse. The school has consulted with parents and the wider community and gained their support for this policy.
Aspect 2 Email, chat, social networking, instant messaging, blogging and video conferencing.	There is no policy relating to the use of communication technologies such as email, chat, social networking, instant messaging, blogging and video conferencing.	A policy relating to the use of communication technologies such as email, chat, social networking, instant messaging, blogging and video conferencing is being developed.	The school has a policy relating to the use of communication technologies such as email, chat, social networking, instant messaging and video conferencing. Users understand that use of these systems will be monitored.	The school has clearly understood and accepted policies relating to the use of communication technologies such as email, chat, social networking, instant messaging and video conferencing. Users understand that use of these systems will be monitored. They understand the risks associated with the use of these devices and are encouraged to be responsible users, both inside school (if allowed) and outside school. The school realises the educational potential of newer communication systems (eg social networking)and is investigating how they might be used safely in school.	The school has clearly understood and accepted policies relating to the use of communication technologies, by staff and students / pupils, such as email, chat, social networking, instant messaging and video conferencing. Users understand that use of these systems will be regularly monitored, with findings reported to the e-safety committee. They understand the risks associated with the use of these systems. The school has realised the educational potential of the newer communications systems and has allowed their safe use within school, where this is relevant to the learning that is taking place. There are clear and enforced sanctions for misuse. The school has consulted with parents and the wider community and gained their support for this policy.

- What evidence could you use?**
- Acceptable Use Policies
 - Home-school agreements
 - Policy for the use of mobile phones / hand held devices
 - Schemes of work and lesson plans
 - Consultation with parents / surveys

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

Element 1 of 4

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

Element A Policy and Leadership - Strand 3 - Communications and Communications Technologies (aspects 3 and 4)

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

ELEMENT A

Policy & Leadership

STRAND 3

Communications and Communications Technologies

	Level 5	Level 4	Level 3	Level 2	Level 1
Aspect 3 Digital and video images	There is no policy relating to the use and publication of digital and video images.	A policy relating to the use and publication of digital and video images is being developed.	The school has policies relating to the use and publication of digital and video images and this is referred to in AUPs.	The school has clearly understood and accepted policies and AUPs relating to the use and publication of digital and video images. Parental permission forms are included in the AUP for publication of images on the website and other publications. Similar permission is gained from older secondary age students, reflecting their personal rights. All members of the school, including staff are educated about the risks associated with the taking, use, sharing, publication and distribution of images (and in particular the risks attached to publishing their own images on the internet). Digital images are always stored securely.	The school has clearly understood and accepted policies relating to the use and publication of digital and video images. Parental permission forms are included in the AUP for publication of images on the website and other publications. Similar permission is gained from older secondary age students, reflecting their personal rights. Members of the school are encouraged to use digital and video images to promote the quality of their learning, but are also educated about the risks associated with the taking, use, sharing, publication and distribution of images (and in particular the risks attached to publishing their own images on the internet). Staff are encouraged to use digital and video images to record learning and to celebrate success, but are aware of the need to take care about the nature of the activities being recorded and to avoid the potential for young people to be identified from published images. Digital images are always stored securely.
Aspect 4 Website, Learning Platform and public facing communications.	There is no reference to e-safety on the school's website, learning platform, newsletters etc.	There are limited references to e-safety on the school's website, learning platform, newsletters etc.	The school's public facing communications eg website, learning platform, newsletters etc are used to provide information about e-safety. The school has considered and addressed e-safety issues in the publication of information through these media.	The school encourages the use of public facing communications eg website, learning platform, newsletters etc and these are used to provide information about e-safety and celebrate the school's successes in this field. The school ensures that good practice has been observed in the use of these media eg use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is no risk to members of the school community, through such publications.	The school encourages the use of public facing communications eg website, learning platform, newsletters etc and these are used to provide information about e-safety and celebrate the school's successes in this field and address (and capture) issues relevant to the e-safety of members of the wider community. The school ensures that good practice has been observed in the use of these media eg use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is no risk to members of the school community, through such publications. These policies and practices are regularly reviewed and reinforced. Care is taken to assess e-safety in the use of new communication technologies.

What evidence could you use?

Policy for the use of digital and video images

AUPs (signed)

Newsletters, website, Learning Platform

Schemes of work and lesson plans

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

Element 1 of 4

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

Element A Policy and Leadership - Strand 3 - Communications and Communications Technologies (aspect 5)

Use this self review tool to establish where your school is on the journey towards an effective e-safety strategy.

Additional support material, resources and links to other websites are available on the SWGfL website: www.swgfl.org.uk/

ELEMENT A
Policy & Leadership
STRAND 3
Communications and Communications Technologies

**Aspect 5
Professional standards**

Level 5	Level 4	Level 3	Level 2	Level 1
The school has no policies or protocols in place for the use of new technologies for communications between the staff and other members of the school and wider community.	The school is developing policies and protocols for the use of new technologies for communications between the staff and other members of the school and wider community.	In consultation with the staff, the school has in place policies and protocols for the use of new technologies for communications between the staff and other members of the school and wider community. Staff follow the Professional Standards for Teachers guidance issued by TDA. Users know that monitoring systems are in place.	In consultation with the staff, the school has in place policies and protocols for the use of new technologies for communications between the staff and other members of the school and wider community. Staff follow the Professional Standards for Teachers guidance issued by TDA. 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 (eg school email, VLE etc) and that the communications must be professional in nature.	In consultation with the staff, the school has in place policies and protocols for the use of new technologies for communications between the staff and other members of the school and wider community. Staff follow the Professional Standards for Teachers guidance issued by TDA. Members of staff only use official school systems (eg school email, VLE etc) for communication with young people, parents / carers and members of the community. Monitoring shows that the culture of the school is reflected in the highly professional nature and content of these communications. The school encourages the use of new communication technologies, but ensures that e-safety issues have been carefully considered and policies updated before they are adopted for use.

What evidence could you use?

Policy documents

Staff handbook

Moving forward – the school might wish to consider: Has the school conducted wide ranging consultation to encourage professional debate and understanding about these issues? Has the school realised the educational potential of the new technologies and encouraged their use, where relevant, while ensuring that staff are protected from potential allegations relating to professional standards?

Element 2 of 4

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

Element B - Infrastructure - Strand 1 - Passwords

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

ELEMENT B

Infrastructure

STRAND 1

Passwords

**Aspect 1
Password security**

Level 5	Level 4	Level 3	Level 2	Level 1
There is no agreed password policy.	Password policies are being developed.	The school has a password policy which applies to all users. Passwords are secure and are consistent with Becta and Local Authority Information Security guidance.	The school has clearly understood and accepted policies relating to the use of passwords. Passwords are secure and consistent with Becta and Local Authority Information Security guidance. Password changes are regularly enforced. Users understand that passwords must never be shared. There are clear procedures for the provision of new passwords, with forced changes at first log-in. All users have clearly defined access rights to school ICT systems. There are clear policies for the use and control of the "master / administrator" passwords.	The school has clearly understood and accepted policies relating to the use of passwords. Passwords are secure and fully compliant with Becta and Local Authority Information Security guidance, with rigorous testing against these standards. Password changes are regularly enforced. Users understand that passwords must never be shared. There are clear procedures for the provision of new passwords, with forced changes at first log-in. All users have clearly defined access rights to school ICT systems. There are clear policies for the use and control of the "master / administrator" passwords. There are regular audits of user log ins to check for anonymous or unauthorised log ins. There is regular testing of systems to ensure that the password security policy is being correctly implemented.

What evidence could you use?

Password security policy

Logs and audits

Home-school agreement

Staff Handbook

Moving forward – the school might wish to consider: How does the school ensure that users understand and accept the importance of password security and follow the school's password security policy, using strong passwords that are changed regularly. Is the school aware of, and reviewing practice as a result of, comprehensive recent guidance from Becta on Information Management and data security?

Element 2 of 4

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

Element B - Infrastructure - Strand 2 - Services Aspects 1 & 2

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

ELEMENT B

Infrastructure

STRAND 2

Services

	Level 5	Level 4	Level 3	Level 2	Level 1
Aspect 1 Filtering	There is no filtering in place.	The school's internet service is not provided by a fully accredited ISP, but filtering is in place.	The school's internet service is provided by a fully accredited ISP. Accredited filtering is in place.	The school's internet service is provided by a fully accredited ISP. Accredited filtering is in place. The school has provided enhanced user level filtering. Differential filtering is being investigated to encourage responsible use and apply sanctions for misuse. The school has monitoring in place to complement the filtering. The school has a monitoring process and takes action when breaches of the filtering policy are revealed. There is a clear route for reporting and managing changes to the filtering system.	The school's internet service is provided by a fully accredited ISP. Accredited filtering is in place. The school has provided enhanced user level filtering. Differential filtering is in place to reward and encourage responsible use as well as sanctions for misuse. The school has monitoring in place to complement the filtering. The school keeps and carries out daily monitoring of the filtering logs and takes action when breaches of the filtering policy are revealed. There is a clear policy concerning requests for and records of changes to the filtering system, with adequate separation of responsibilities and regular oversight by senior leaders. Evidence from monitoring and filtering logs shows that users have a mature approach and that there are very few incidents of misuse. The school is therefore able to take an appropriate and balanced approach to filtering, in the knowledge that users have adopted safe on-line behaviour.
Aspect 2 Technical security	The school does not meet the e-safety technical requirements outlined in regional (eg SWGfL) and Local Authority Security Policies and Acceptable Usage Policies.	The school meets the e-safety technical requirements outlined in regional (eg SWGfL) and Local Authority Security Policies and Acceptable Usage Policies.	The school's public facing communications eg website, learning platform, newsletters etc are used to provide information about e-safety. The school has considered and addressed e-safety issues in the publication of information through these media.	The school meets the e-safety technical requirements outlined in regional (eg SWGfL) and Local Authority Security Policies and Acceptable Usage Policies. There are regular reviews and audits of the safety and security of school ICT systems, with oversight from senior leaders and these have impact on policy and practice. The school's ICT infrastructure is secure and is not open to misuse or malicious attack.	The school meets the e-safety technical requirements outlined in regional (eg SWGfL) and Local Authority Security Policies and Acceptable Usage Policies. There are regular reviews and audits of the safety and security of school ICT systems with oversight from senior leaders and these have impact on policy and practice. Internal reviews are augmented by rigorous external reviews of the security of school systems. School practice reflects up to date advancements in security, providing protection from new security threats as they arise.

What evidence could you use?

Filtering Policy

Monitoring logs and audits

Review documents (internal and external)

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

Element 2 of 4

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

Element B - Infrastructure - Strand 2 - Services Aspect 3

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

ELEMENT B
Infrastructure
STRAND 2
Services

**Aspect 3
Personal data**

Level 5	Level 4	Level 3	Level 2	Level 1
There is no agreed Personal Data policy.	A Personal Data policy is being developed.	The school has a Personal Data policy. All staff know and understand the need to ensure the safe keeping of personal data, minimising the risk of its loss or misuse. (Adhering to the Data Protection Act and relevant Becta guidance). Parents and carers are informed about their rights and about the use of personal data through the Privacy Notice (formerly Fair Processing Notice).	The school has a Personal Data policy. All staff know and understand the need to ensure the safe keeping of personal data, minimising the risk of its loss or misuse. (Adhering to the Data Protection Act and relevant Becta guidance). Clear policies about the secure handling, transfer and disposal of data (passwords, encryption, and removable media) are known, understood and adhered to by users. Parents and carers are informed about their rights and about the use of personal data through the Privacy Notice (formerly Fair Processing Notice). Password protection is enhanced by the use of encryption and / or two factor authentication for the handling or transfer of sensitive data. The school has appointed a Senior Risk Information Officer / Data Protection Officer and Information Asset Owners.	The school has a Personal Data policy. Staff know and understand the need to ensure the safe keeping of personal data, minimising the risk of its loss or misuse. (Adhering to the Data Protection Act and relevant Becta guidance). Clear policies about the secure handling and transfer of data (passwords, encryption, and removable media) are known, understood and adhered to by users. Parents and carers are informed about their rights and about the use of personal data through the Privacy Notice (formerly Fair Processing Notice). Password protection is enhanced by the use of encryption and / or two factor authentication for the handling or transfer of sensitive data. The school has appointed a Senior Risk Information Officer / Data Protection Officer and Information Asset Owners. All protected data is clearly labelled with Impact Labels. There is a clear procedure in place for audit logs to be kept and for reporting, managing and recovering from information risk incidents.

What evidence could you use?

Personal Data Policy

Privacy notice (formerly Fair Processing Notice)

Job descriptions

Moving forward – the school might wish to consider: Is the school confident that policy and good practice ensure that all personal data is safe from risk of loss, misuse and unauthorised access? Are staff aware of their responsibilities? Is the school aware of, and reviewing practice as a result of, comprehensive recent guidance from Becta on Information Management?

Element 3 of 4

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

Element C Education - Strand 1 - Children and Young People Aspects 1 & 2

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

ELEMENT C

Education

STRAND 1

Children and Young People

	Level 5	Level 4	Level 3	Level 2	Level 1
Aspect 1 E-safety education	There is no planned programme of e-safety education.	A planned programme of e-safety education is being developed.	A planned e-safety education programme takes place through PHSE / ICT / other lessons and is regularly revisited. Pupils / students are aware of e-safety issues and are empowered to stay safe. Appropriate e-safety resources are used. The school is aware of the need to educate and protect vulnerable children who may be put at particular risk from their and others' actions on-line.	A planned e-safety education programme takes place through PHSE / ICT / other lessons and across the curriculum, for all children in all years and is regularly revisited. There is breadth and progression. Pupils / students are aware of e-safety issues and understand and follow the e-safety and acceptable use policies. Appropriate e-safety resources are used. The school is effective in the education and protection of vulnerable children who may be put at particular risk from their and others' actions on-line. The school regularly evaluates the effectiveness and impact of e-safety programmes.	A planned e-safety education programme takes place and is fully embedded for all children in all aspects of the curriculum in all years and in other school activities, including extended school provision. There is breadth and progression. The provision is regularly audited, reviewed and revised. Pupils / students are aware of e-safety issues and understand and follow the e-safety and acceptable use policies. E-safety resources are varied and appropriate and use new technologies to deliver e-safety messages in an engaged and relevant manner. Young people are themselves involved in e-safety education eg through peer mentoring. The school is effective in the education and protection of vulnerable children who may be put at particular risk from their and others' actions on-line. The school regularly evaluates the effectiveness and impact of e-safety programmes.
Aspect 2 Information literacy	There are no opportunities for pupils / students to gain an understanding of information literacy skills.	Opportunities for pupils / students to gain an understanding of information literacy skills are being developed.	Pupils / students are taught in some lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information. They have an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.	Pupils / students are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information. Staff and pupils / students use and understand "Creative Commons" licencing. There are many opportunities for them to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.	Pupils / students are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information. Staff and pupils / students use and understand "Creative Commons" licencing. There are many opportunities for them to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. The school actively provides systematic opportunities for pupils / students to develop the skills of safe and discriminating on-line behaviour. Staff and pupils / students acknowledge copyright and intellectual property rights in all their work.

What evidence could you use?

Schemes of work

Lesson plans

Classroom resources

Learning Platform, VLE, website

Work samples, exercise books etc

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

Element 3 of 4

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

Element C Education - Strand 1 - Children and Young People Aspect 3

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

ELEMENT C

Education

STRAND 1

Children and Young People

**Aspect 3
The contribution of young people**

Level 5	Level 4	Level 3	Level 2	Level 1
The school does not acknowledge or use the high level of skills and knowledge of young people in the use of new technologies in its e-safety programmes.	The school is developing opportunities to acknowledge and use the high level of skills and knowledge of young people in the use of new technologies in its e-safety programmes.	The school acknowledges, learns from and uses the high level of skills and knowledge of young people in the use of new technologies. These contribute to the development of e-safety programmes.	The school acknowledges, learns from and uses the high level of skills and knowledge of young people in the use of new technologies. The school involves pupils / students in e-safety campaigns and in peer mentoring, buddying and counselling schemes within the school. Pupils / students are encouraged to provide feedback in reviews of e-safety related policies and AUPs.	The school acknowledges, learns from and uses the high level of skills and knowledge of young people in the use of new technologies. Staff frequently invite pupils / students to contribute through their knowledge and skills. The school involves pupils / students in e-safety campaigns and in peer mentoring, buddying and counselling schemes and as student researchers. Pupils / students are encouraged to provide feedback in reviews of e-safety related policies and AUPs. Young people actively contribute to parents' evenings and family learning programmes with e-safety as their focus.

What evidence could you use?

Peer mentoring programmes

Buddying schemes

Contributions from children and young people in school publications / on school website / at parents' evenings

Moving forward – the school might wish to consider:

Does the school acknowledge and make full use of the contribution that young people as “digital natives” can make to e-safety in and out of school?

Element 3 of 4

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

Element C Education - Strand 2 - Staff Strand 3 Governors

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

ELEMENT C
Education
STRAND 2
Staff
**Aspect 1
Staff training**

Level 5	Level 4	Level 3	Level 2	Level 1
The school does not acknowledge or use the high level of skills and knowledge of young people in the use of new technologies in its e-safety programmes.	There is no formal e-safety training programme for staff. Child Protection / Safeguarding training does not cover e-safety.	A formal e-safety staff training programme is being developed. Child Protection / Safeguarding training will cover e-safety.	A planned programme of formal e-safety training is made available to all staff. E-safety training is an integral part of Child Protection / Safeguarding training and vice versa. An audit of e-safety training needs is carried out regularly and is addressed in Performance Management targets. All staff have an up to date awareness of e-safety matters, current school e-safety policy and practices and child protection / safeguarding procedures. All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy. Staff are working toward the European Pedagogical ICT Licence (EPICT) E-Safety Certificate or equivalent.	A planned programme of formal e-safety training is made available to all staff. E-safety training is an integral part of Child Protection / Safeguarding training and vice versa. An audit of e-safety training needs is carried out regularly and is addressed in Performance Management targets. All staff have an up to date awareness of e-safety matters, the current school e-safety policy and practices and child protection / safeguarding procedures. All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy. The culture of the school ensures that staff support each other in sharing knowledge and good practice about e-safety. The school takes every opportunity to research and understand good practice that is taking place in other school. A range of staff have gained the European Pedagogical ICT Licence (EPICT) E-Safety Certificate or equivalent.

STRAND 3
Governors
**Aspect 1
Governor training**

Level 5	Level 4	Level 3	Level 2	Level 1
Governors do not receive e-safety awareness training.	E-safety awareness training for Governors is being developed.	E-Safety awareness training is provided for Governors (either in or out of school).	E-Safety awareness training is provided for Governors. A nominated E-Safety Governor has received training and is responsible for providing e-safety information to other Governors.	E-Safety awareness training is provided for Governors. Governors have made a commitment to e-safety training and a number of Governors have taken part.

What evidence could you use?

Staff training needs analysis

Staff training programmes

CPD portfolios

Induction programmes

Good practice visits / Learning walks

Governor training records

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

Element 3 of 4

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

Element C Education - Strand 4 Parents/Carers - Strand 5 Community/Extended Schools

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

ELEMENT C
Education
STRAND 4
Parents and Carers
**Aspect 1
Parental
education**

Level 5	Level 4	Level 3	Level 2	Level 1
The school does not provide opportunities for parents to receive education or information about e-safety.	The school is developing opportunities for parents to receive education or information about e-safety.	The school provides opportunities for parents to receive education or information about e-safety. Parents and carers are aware of and endorse (by signature) the Pupil / Student Acceptable Use Policy. All parents have received a copy of Know it all (or equivalent).	The school provides opportunities for parents to receive regular education or information about e-safety. Parents and carers are aware of and endorse (by signature) the Pupil / Student Acceptable Use Policy. All parents have received a copy of Know it all (or equivalent) .The school understands the importance of the role of parents and carers in e-safety education and in the monitoring / regulation of the children's on-line experiences (particularly out of school). Parents and carers know who to contact if they are worried about e-safety issues.	The school provides opportunities for parents to receive regular education or information about e-safety. Parents and carers are aware of and endorse (by signature) the Pupil / Student Acceptable Use Policy. All parents have received a copy of Know it all (or equivalent). The school understands the importance of the role of parents and carers in e-safety education and in the monitoring / regulation of the children's on-line experiences (particularly out of school). Parents and carers know who to contact if they are worried about e-safety issues. The school takes every opportunity to help parents and carers understand e-safety issues through parents' evenings, newsletters, website, VLE etc. Parents and carers know about the school's complaints procedure and how to use it effectively. The school is effective in engaging "hard to reach" parents in e-safety programmes.

STRAND 5
Community - Extended Schools
**Aspect 1
Community
understanding**

Level 5	Level 4	Level 3	Level 2	Level 1
The school does not provide opportunities for members of its wider community to gain information and understanding about e-safety.	The school is developing opportunities for members of its wider community to gain information and understanding about e-safety.	The school provides opportunities for members of its wider community to gain information and understanding about e-safety.	The school provides opportunities for members of its wider community to gain information and understanding about e-safety. Family learning courses are offered in ICT, media literacy and e-safety. Plans are being developed to increase community involvement.	The school provides opportunities for members of its wider community to gain information and understanding about e-safety. Family learning courses are offered in ICT, media literacy and e-safety. 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.

What evidence could you use?

Acceptable Use Policies

Letters to parents, newsletters, website

Parents' evenings / courses

Family learning events

Moving forward – the school might wish to consider: Does the school acknowledge the importance of parents and carers in e-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? Does the school also provide this service to other members of the community, through its extended services?

Element 4 of 4

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

Element D Standards and Inspection - Strand 1 Monitoring

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

ELEMENT D

Standard and Inspection

STRAND 1

Monitoring

	Level 5	Level 4	Level 3	Level 2	Level 1
Aspect 1 Monitoring and Reporting on E-Safety Incidents	There is no monitoring of e-safety incidents.	Monitoring of e-safety incidents is being developed.	Monitoring of e-safety incidents takes place and records are kept. The records are reviewed / audited and reported to the school's senior leaders. Parents are informed of e-safety incidents, as relevant.	Monitoring and recording of e-safety incidents takes place. The records are reviewed / audited and reported to the school's senior leaders, Governors, the Local Authority and the Local Children's Safeguarding Board (LSCB) E-Safety Sub Committee. Monitoring and reporting of incidents contributes to developments in policy and practice in e-safety within the school. Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible. All parents / carers are informed of patterns of e-safety incidents as part of the school's e-safety awareness raising.	Monitoring and recording of e-safety incidents takes place. The records are reviewed / audited and reported to the school's senior leaders, Governors, the Local Authority and the Local Children's Safeguarding Board (LSCB) E-Safety Sub Committee. Monitoring and reporting of incidents contributes to developments in policy and practice in e-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 e-safety strategy. Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible. All parents / carers are informed of patterns of e-safety incidents as part of the school's e-safety awareness raising.
Aspect 2 Monitoring the impact of the e-safety policy and practice	There is no monitoring of the impact of the e-safety policy and practice.	Monitoring of the impact of the e-safety policy and practice is being developed.	The impact of the e-safety policy and practice is monitored through the review / audit of e-safety incident logs, behaviour / bullying logs, surveys of staff, students / pupils, parents / carers.	The impact of the e-safety policy and practice is monitored through the review / audit of e-safety incident logs, behaviour / bullying logs, surveys of staff, students / pupils, parents / carers. The school reviews the effectiveness of e-safety support received from external agencies. There is balanced professional debate about the evidence taken from the data ie the logs/ audits and the impact of preventative work ie e-safety education, awareness and training.	The impact of the e-safety policy and practice is monitored through the review / audit of e-safety incident logs, behaviour / bullying logs, surveys of staff, students / pupils, parents / carers. The school reviews the effectiveness of e-safety support received from external agencies. There is balanced professional debate about the evidence taken from the data ie the logs / audits and the impact of preventative work ie e-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 e-safety strategy.

What evidence could you use?

Incident logs and audits / reviews

School Improvement Plan

Self Evaluation documents – particularly SEF section 4b

Minutes of meetings of relevant groups, and committees, including Governors

Monitoring reports

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



School E-Safety Self Review Tool

R1

Record Sheet 1

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

360 degree safe School E-Safety Self Review Tool (E-Safety Mark benchmark levels are shaded in red)

ELEMENT A

Policy and Leadership

STRAND 1

Responsibilities

Level 5

Level 4

Level 3

Level 2

Level 1

Comment

Sources of Evidence

Aspect 1 E-Safety Committee							
Aspect 2 E-safety responsibilities							
Aspect 3 Governors							

STRAND 2

Policies

Aspect 1 Policy development							
Aspect 2 Policy scope							
Aspect 3 Acceptable Use Policies							
Aspect 4 Self Evaluation							
Aspect 5 Whole School							
Aspect 6 Sanctions							
Aspect 7 Reporting							

School E-Safety Self Review Tool

Record Sheet 2

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

ELEMENT A

Policy and Leadership

STRAND 3

Communications and Communications Technology

Level 5
Level 4
Level 3
Level 2
Level 1
Comment
Sources of Evidence

	Level 5	Level 4	Level 3	Level 2	Level 1	Comment	Sources of Evidence
Aspect 1 Mobile phones and personal hand held devices							
Aspect 2 Email, chat, social networking, instant messaging, blogging, video conferencing							
Aspect 3 Digital and video images							
Aspect 4 Website, Learning Platform, public facing communications							
Aspect 5 Professional standards							

ELEMENT B

Infrastructure

STRAND 1

Passwords

	Level 5	Level 4	Level 3	Level 2	Level 1	Comment	Sources of Evidence
Aspect 1 Password security							

STRAND 2

Services

	Level 5	Level 4	Level 3	Level 2	Level 1	Comment	Sources of Evidence
Aspect 1 Filtering							
Aspect 2 Technical security							
Aspect 3 Personal data							



LSCB E-Safety Self Review Tool

R4

Record Sheet 4

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

ELEMENT D

Standards and Inspection

STRAND 2

Monitoring

Level 5

Level 4

Level 3

Level 2

Level 1

Comment

Sources of Evidence

Aspect 1
Monitoring and Reporting on E-Safety Incidents

Aspect 2
Monitoring the impact of the e-safety policy and practice

Name of School	<input type="text"/>
Contact Person	<input type="text"/>
School Address	<input type="text"/>
Email Address	<input type="text"/>
Telephone Number	<input type="text"/>