LSCB E-Safety Self Review Tool

LSCB E-Safety Self Review Tool

Contents

Introduction

The development and expansion of the use of on-line and mobile technologies, and particularly of the internet, has transformed society in recent years. ICT is an important educational tool, while children and young people routinely use ICT to communicate with themselves and others. Many recreational activities now encompass the use of ICT and increasingly there is convergence between the offline and online worlds. Children and young people generally have high level ICT skills, often in advance of those of their parents, carers and other adults.

It is recognised that the benefits that ICT can bring to young people are perceived to "outweigh the risks." However, all organisations that work with children and young people must, through their e-safety policy and practice, ensure that they meet their statutory obligations to ensure that children and young people (and staff and volunteers) are safe and are protected from potential harm. Ensuring that children and young people are able to use the internet and related communications technologies appropriately and safely is part of the wider duty of care to which all who work with children and young people are bound. E-safety policies should help to ensure safe and appropriate use and should address both technical solutions and education and awareness. The development and implementation of an LSCB e-safety strategy should involve all agencies that work with children, young people and their families and best practice suggests that they should also involve the young people and their parents and carers.

This Self Review Tool is intended to help the LSCB to review its e-safety policy and practice and provide:

- Management information that can influence the production or review of an LSCB e-safety strategy, e-safety policies and develop good practice
- A process for identifying strengths and weaknesses
- Opportunities for commitment and involvement from all member agencies
- A continuum for the LSCB to discuss how it might move from a basic level of e-safety provision to practice that is aspirational and innovative.

LSCBs may wish to recommend to member agencies that they should use other 360 degree safe self review tools to review their own practice: www.360safe.org.uk (for schools) and www.swgfl.org.uk/osp - the Online Safety Planner (for other organisations that work with children and young people).

LSCB E-Safety Self Review Tool

The self review tool enables you to review your LSCB's current practice in e-safety over four main elements, based on the Becta PIES model:

A. POLICY & LEADERSHIP   **B. INFRASTRUCTURE**   **C. EDUCATION & TRAINING**   **D. STANDARDS & INSPECTION**

Each element includes a number of strands, which in turn include a number of aspects. Organisations may choose to work through the tool in the order that is offered, or may alternatively take elements, strands or aspects individually to suit their own circumstances.

Each aspect has statements at five levels of maturity which range as below:

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

A record sheet is attached, on which LSCBs can identify, for each aspect, the level that matches their current practice. By reading the higher level descriptors, it will be possible to identify the steps that are needed to progress further.

The record sheet also includes sections for comments – which organisations 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 to share knowledge and information among those involved in the review. It may also be helpful to any external consultant or adviser that the LSCB or member agency might wish to involve in its audit, review or policy development.

It is suggested that the LSCB should use a multi-agency 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 representatives of member organisations should be engaged in the process to ensure understanding and ownership.

Once the LSCB's current position has been established, the findings can then be used to draw up an action plan for development.

LSCB E-Safety Self Review Tool

Links to documents and resources

Becta - **"Safeguarding Children in a Digital World" - Developing an LSCB E-Safety Strategy**
http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_tl_rs_03&rid=13344

"Safeguarding children online: a checklist for local authorities and local safeguarding children boards"
http://localauthorities.becta.org.uk/index.php?section=pb&catcode=la_pub_01&rid=13100

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

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

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 and communities will be the "School E-Safety Policy Template".
360 degree safe Online Self Review Tool for schools - www.360safe.org.uk
Online Safety Planner (for organizations that work with children and young people) www.swgfl.org.uk/osp

UK Council for Internet Child Safety: http://www.dcsf.gov.uk/ukccis/

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 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.

LSCB 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.

South West Grid For Learning Self Review Framework

ELEMENT A — Policy & Leadership

STRAND 1 — Responsibilities

	Level 5	Level 4	Level 3	Level 2	Level 1
Aspect 1 E-Safety Sub group	There is no LSCB e-safety sub group.	The LSCB is developing an e-safety sub group.	The LSCB has an e-safety sub group with a clear brief and representation from a range of agencies.	The LSCB has an active e-safety sub group. Wide representation from all relevant member agencies is clearly defined in the agreed terms of reference. It has clear lines of responsibility and accountability. There is an appointed E-Safety Board Member who is a member of the e-safety group. There is ownership by the core / mandatory member agencies.	The LSCB has an active e-safety sub group. Wide representation from all relevant member agencies is clearly defined in the agreed terms of reference. It has clear lines of responsibility and accountability which are understood by all member agencies. It is chaired by a member of the LSCB. There is clear ownership by all member agencies.
Aspect 2 E-safety responsibilities	No one has responsibility for e-safety in / on the LSCB.	Some member agencies have a person with responsibility for e-safety but there is little co-ordination of their work across the LSCB. No one has responsibility for e-safety in / on the LSCB.	The LSCB has a designated person responsible for co-ordinating the work of the e-safety sub group. The core member agencies each have a person responsible for e-safety. The LSCB designated person is aware of the e-safety work of the core member agencies. There is some co-ordination.	The LSCB has a designated person responsible for co-ordinating the work of the e-safety sub group. All member agencies have a designated person responsible for e-safety. There are clear lines of responsibility and accountability and member agencies understand their respective responsibilities, particularly in responding to specific e-safety incidents.	The LSCB has a designated person responsible for co-ordinating the work of the e-safety sub group. All member agencies have a designated person responsible for e-safety. There are clear lines of responsibility and accountability and member agencies understand their respective responsibilities, particularly in responding to specific e-safety incidents. There is ownership of an LSCB wide programme of e-safety awareness raising, education and training.

What evidence could you use?

LSCB vision and aims

Action / Business Plans

Self Evaluation documents

Job / role descriptions

Minutes of meetings of relevant groups and committees.

E-Safety Strategy

Moving forward – the LSCB might wish to consider:
How to engage ALL member agencies, and all those working in the member agencies, in the work of e-safety sub group. Is there ownership of the group and its work by member agencies? Do all stakeholders know, understand and accept their responsibilities?

LSCB 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 & Leadership				
STRAND 1	**Responsibilities**				

	Level 5	Level 4	Level 3	Level 2	Level 1
Aspect 3 **LSCB (the parent body)**	There is no involvement in e-safety by the Board or its members.	Board members are aware that an e-safety policy is being developed, but they are not involved in its development.	Board members are involved in the development and approval of the e-safety policy.	Board members are involved in the development and approval of the e-safety policy. There is an appointed E-Safety Board Member who is a member of the e-safety sub group. Board members are aware of their responsibilities with regard to e-safety. The Board allocates resources to e-safety.	Board members are involved in the development and approval of the e-safety policy. The e-safety sub group is chaired by a Board member. All Board members are aware of their responsibilities with regard to e-safety. The Board receives regular monitoring reports on the implementation of the e-safety policy and on reported incidents. Board members are involved in the promotion of e-safety across member agencies and in the wider community.

STRAND 2	**Policies**				

	Level 5	Level 4	Level 3	Level 2	Level 1
Aspect 1 **Strategy development**	There is no LSCB e-safety strategy.	The LSCB is developing an e-safety strategy.	The LSCB has an e-safety strategy, aligned with national, regional and LA policies. The strategy has resulted in an Action Plan being developed.	The LSCB has an e-safety strategy, which is aligned with national, regional and LA policies and has been developed in consultation with a wide range of member agencies. There is "LSCB wide ownership" of the strategy. The strategy is reviewed annually. The strategy has resulted in an effective Action Plan being developed.	The LSCB has an e-safety strategy which is aligned with national, regional and LA policies and has been developed in consultation with all member agencies and the wider community. There is full ownership of the strategy. The strategy is reviewed annually and more frequently in light of changes in technology or e-safety incidents. The strategy and the resulting Action Plan are embedded within the wider LSCB business planning process.
Aspect 2 **E-safety policies**	Member agencies do not have e-safety policies.	Member agencies are developing e-safety policies.	Core member agencies have e-safety policies. These are being developed by other member agencies.	All member agencies have e-safety policies. The LSCB E-Safety Sub Group has audited and reviewed these policies and is confident that policy and practice in member agencies is consistent and effective.	All member agencies have e-safety policies. The LSCB E-Safety Sub Group has audited and reviewed these policies and is confident that policy and practice in member agencies is consistent and effective. The effectiveness of these policies is regularly monitored and reviewed by each member organisation. All policies are updated in the light of the ongoing development of new technologies which may put young people at risk.

What evidence could you use?

E-Safety Policies

Minutes of the LSCB and the E-Safety Sub Group (and other relevant groups)

Information for users – letters, newsletter, website etc

Acceptable Use Policies

Review documents

LSCB reports to Children's Trust

Moving forward – the LSCB might wish to consider:
How to engage ALL member agencies in the work of e-safety sub group and in the establishment and review of e-safety policies. How the member agencies 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 organisational culture.

LSCB 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.

	Policy & Leadership				
ELEMENT A					
STRAND 2	**Policies**				
	Level 5	**Level 4**	**Level 3**	**Level 2**	**Level 1**
Aspect 3 **Programme of Work (Action Plan)**	There is no LSCB / E-Safety Sub Group Programme of Work.	An LSCB / E-Safety Sub Group Programme of Work is being developed. An audit of policy and practice across member agencies is being carried out / has been carried out.	An LSCB / E-Safety Sub group Programme of Work has been developed, in consultation with member agencies. An audit of policy and practice across member agencies has been carried out and has influenced the Programme of Work.	The LSCB / E-Safety Sub group Programme of Work, developed, in consultation with member agencies, is detailed and prioritised and includes clear and accountable actions and a timeline for achieving key milestones.	The LSCB / E-Safety Sub group Programme of Work, developed, in consultation with member agencies, is detailed and prioritised and includes clear and accountable actions and a timeline for achieving key milestones. The effectiveness of its outputs are regularly monitored and reviewed. There is effective co-ordination of programmes of work across member agencies.
Aspect 4 **Acceptable Use Policies**	Member agencies do not have Acceptable Use Policies.	Member agencies are developing Acceptable Use Policies.	Core member agencies have Acceptable Use Policies. These are being developed by other member agencies.	All member agencies have Acceptable Use Policies in place for all users, and are signed by all users. There are clear induction policies to ensure that young people and adults who are new to the agencies are informed of and required to sign AUPs.	All member agencies have Acceptable Use Policies, which are differentiated by age and stage and are in place for and are signed (annually) by all users. There are clear induction policies to ensure that young people and adults who are new to the agencies 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.
Aspect 5 **Embedding policy and practice**	Member agencies do not address e-safety in their wider policies and practice.	Member agencies are beginning to address e-safety in their wider policies and practice.	Member agencies address e-safety in their wider policies and practice.	There are clear and consistent links between the member agencies' e-safety policies and practice and sections of other policies where there is reference to e-safety eg in the behaviour, anti-bullying, PHSE, Child Protection / Safeguarding, ICT and employment policies.	E-safety is embedded in the relevant policies and practice of member agencies. They have carefully considered their approach to e-safety and provide a consistent e-safety message to all members of their organisation and, where relevant, the wider community. This is particularly apparent in the references to e-safety within such policies as the behaviour, anti-bullying, PHSE, Child Protection / Safeguarding, ICT and employment policies.

What evidence could you use?

Self evaluations

Inspection / Audit reports

Independent audits

LA and other external reviews Induction policies

Member agency policies eg anti-bullying, Child Protection, ICT and Employment

Child Protection Procedures

Moving forward – the LSCB might wish to consider:
How effective are self evaluation processes and procedures? To what extent do member agencies regarded e-safety as an issue for the whole organisation, rather than just the responsibility of one section, eg the ICT department. To what extent is e-safety regarded as a child welfare / safeguarding 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 & Leadership

STRAND 2 — Policies

What evidence could you use?

Codes of conduct

Behaviour and anti-bullying policies

Rewards and sanctions policies

Publicity materials

Incident logs with evidence of monitoring and auditing

	Level 5	Level 4	Level 3	Level 2	Level 1
Aspect 6 Reporting (in member agencies)	In member agencies, users are unclear about their responsibilities to report e-safety incidents and allegations. There is no clear process for reporting abuse.	In member agencies, systems and processes are in place for users to report e-safety incidents and allegations. These are not yet consistently understood or consistently used.	In member agencies, with reporting systems in place, users understand their responsibilities to report e-safety incidents and allegations. 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 and allegations. Reports are logged for future auditing / monitoring.	In member agencies, with reporting systems in place, users 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. Agencies actively seek support from the local authority, the police and other relevant bodies in dealing with e-safety issues.	In member agencies, there are clearly known and understood systems for reporting e-safety incidents and allegations and these are used effectively. The culture of each organisation encourages all its members and, where relevant, its wider community to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through escalation processes. Reports are logged and regularly audited and monitored. Agencies actively seek support from the local authority, the police and other relevant bodies, with whom there are effective links, in dealing with e-safety issues. These help the organisation and, where relevant, members of the wider community in dealing with e-safety issues.
Aspect 7 Dealing with e-safety incidents and sanctions for misuse (in member agencies)	In member agencies there are no clear processes for dealing with incidents. There are no sanctions for e-safety abuse or misuse.	In member agencies there are processes for dealing with incidents and there are sanctions for e-safety abuse or misuse, but these are not linked to an agreed policy / AUP and are not consistently enforced.	In member agencies there are processes for dealing with incidents and there are sanctions for e-safety abuse or misuse. These are clearly stated in the e-safety policies and users are aware of them.	In member agencies there are processes for dealing with incidents and there are sanctions for e-safety abuse or misuse. These are clearly stated in the e-safety policies. Users are aware of the processes for dealing with incidents and aware of the sanctions, understand their importance and generally adhere to the e-safety policy.	In member agencies, both the processes for dealing with incidents and also the sanctions for e-safety abuse or misuse are clearly stated in the e-safety policy. Users are aware of these and understand their importance. At most, only a few users fail to adhere to the e-safety policy. The organisation is strict in monitoring and applying the e-safety policy and a differentiated and appropriate range of sanctions. Users understand the clear policy of the organisation that sanctions can be applied to e-safety incidents that take place outside the organisation, if they are related to that organisation.

Moving forward – the LSCB might wish to consider:
Do users (young people and staff / volunteers) 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?

LSCB 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 & Leadership				
STRAND 3	Communications and Communications Technologies				
	Level 5	Level 4	Level 3	Level 2	Level 1
Aspect 1 Communications technologies eg mobile phones, email, chat, social networking, video conferencing, websites, and the use of digital and video images	In member agencies, e-safety and related policies do not cover the use of these communications technologies.	In member agencies, e-safety and related policies are being developed to cover the use of these communications technologies.	In member agencies the use of these communications technologies is covered in the organisation's e-safety or related policies.	Member agencies have clearly understood and accepted policies relating to the use of these communications technologies. Users understand the risks associated with their use and are encouraged to be safe and sensible users. Agencies working with young people recognise the educational potential of these technologies and are encouraging, where relevant, the safe use of these technologies.	Member agencies have clearly understood and accepted policies relating to the use of these communications technologies. Users have a mature approach to their safe use. Agencies working with young people have recognised the educational potential of these technologies and have allowed / encouraged their safe use, where this is relevant. There are clear and enforced sanctions for misuse.
Aspect 2 LSCB E-Safety Communications Plan	The LSCB E-Safety Group has no Communications Plan.	The LSCB E-Safety Group is developing a Communications Plan.	The LSCB E-Safety Group has a Communications Plan.	The LSCB E-Safety Group has a Communications Plan. There is effective communication and co-ordination between the LSCB and its E-Safety Sub group and between the E-Safety Sub group and the member agencies.	The LSCB E-Safety Group has a Communications Plan. There is effective communication and co-ordination between the LSCB and its E-Safety Sub group and between the E-Safety Sub group and the member agencies. There is ownership of the E-Safety Sub group Communications Plan by the LSCB and by member agencies.

What evidence could you use?

Acceptable Use Policies

Policy for the use of mobile phones / hand held devices / new communications technologies

LSCB Consultation with member agencies

Member agencies consultation with users

Moving forward – the LSCB might wish to consider:
How are member agencies ensuring the safe use of these technologies, for all children within the local area, both within their organisations (where allowed) and in the wider community, where there may be serious issues about use that is not monitored or regulated? Have member agencies realised and are they exploiting the educational potential of these technologies and considered how their safe use might be encouraged, where relevant?

LSCB 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 & Leadership				
STRAND 3	Communications and Communications Technologies				

	Level 5	Level 4	Level 3	Level 2	Level 1
Aspect 3 **Awareness Raising**	The E-Safety Sub group has no policy or process for e-safety awareness raising.	The E-Safety Sub group is developing a policy and processes for e-safety awareness raising.	The E-Safety Sub group is actively raising awareness of e-safety through communications with member agencies and with children and young people, parents and carers and with the media.	The E-Safety Sub group is actively raising awareness of e-safety through communications with member agencies and with children and young people, parents and carers and with the media. The views of children and young people and of parents and carers are taken into account and consideration is given as to how they may be given a measure of choice and control in the development of services.	The E-Safety Sub group is actively raising awareness of e-safety through communications with member agencies and with children and young people, parents and carers and with the media. The views of children and young people and of parents and carers are taken into account and consideration is given as to how they may be given a measure of choice and control in the development of services. A shared responsibility is promoted, increasing the effectiveness of local education and training strategies.
Aspect 4 **Media Strategy**	The E-Safety Sub group has no media strategy.	The E-Safety Sub group is developing a media strategy.	The E-Safety Sub group has a media strategy. The Sub group and member agencies have procedures in place for reacting to and dealing with the media in the event of e-safety incidents taking place.	The E-Safety Sub group has a media strategy. The Sub group and member agencies have procedures in place for reacting to and dealing with the media in the event of e-safety incidents taking place. A nominated person is in place to deal with the media. Effective relationships have been developed with the media and this has resulted in positive e-safety messages being published.	The E-Safety Sub group has a media strategy. The Sub group and member agencies have procedures in place for reacting to and dealing with the media in the event of e-safety incidents taking place. A nominated person is in place to deal with the media. Effective relationships have been developed with the media and this has resulted in positive e-safety messages being published. Media training / information is provided for member agencies. There is media representation on the E-Safety Sub group.

What evidence could you use?

Newsletters, websites, publicity materials

Consultation with young people and with parents and carers

Job descriptions

Media coverage

Conference / CPD records

Moving forward – the LSCB might wish to consider:
How are the LSCB and member agencies raising awareness of e-safety in the local area? Has the LSCB media strategy been successful in gaining positive publicity for e-safety awareness raising campaigns? Are member agencies adequately prepared to deal, in a balanced way, with media interest in serious incidents that might arise?

LSCB 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 & Leadership
STRAND 3	Communications and Communications Technologies

Aspect 5 Professional standards (Staff and volunteers)

Level 5	Level 4	Level 3	Level 2	Level 1
In member agencies the use of new technologies for communications between adults and young people is not covered in policies or protocols.	Member agencies are developing policies and protocols to cover the use of new technologies for communications between adults and young people. Some member agencies have these in place.	Member agencies have policies and protocols to cover the use of new technologies for communications between adults and young people. Staff follow their relevant Professional Standards. Users know that monitoring systems are in place. Relevant national guidelines and codes of practice are observed.	Member agencies have policies and protocols to cover the use of new technologies for communications between adults and young people. Staff follow their relevant Professional Standards. Users know that monitoring systems are in place. Members of staff understand the need for communication with young people, parents / carers and members of the community to take place only through official communications systems (eg official email) and that the communications must be professional in nature. Relevant national guidelines and codes of practice are observed.	Member agencies have policies and protocols to cover the use of new technologies for communications between adults and young people. Staff follow their relevant Professional Standards. Users know that monitoring systems are in place. Members of staff understand the need for communication with young people, parents / carers and members of the community to take place only through official communications systems (eg official email) and that the communications must be professional in nature. Monitoring shows that the culture of member agencies is reflected in the highly professional nature and content of these communications. The agencies encourage the use of new communication technologies but ensure that e-safety issues have been carefully considered and policies updated before they are adopted for use. Relevant national guidelines and codes of practice are observed.

What evidence could you use?

Codes of conduct

Policy documents

Staff handbooks

Induction policies and procedures

Moving forward – the LSCB might wish to consider:
Have member agencies conducted wide ranging consultation to encourage professional debate and understanding about these issues? Have member agencies 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?

LSCB E-Safety Self Review Tool

Element 2 of 4 — This element reflects the importance of having effective systems in place to ensure the security of 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	Services				
	Level 5	**Level 4**	**Level 3**	**Level 2**	**Level 1**
Aspect 1 Filtering	Some internet access for children within the Local Authority is unfiltered.	Internet access in schools is filtered, although this may not be from an accredited service provider. Other access for children within the LA is not filtered (eg. Youth service, foster carers).	Internet access in schools is provided by a fully accredited ISP. Accredited filtering is in place. All internet access for children and young people within the LA is filtered, although the filtering is not necessarily monitored and not necessarily delivered by a fully accredited ISP – there may be no checks to see that it is actually being deployed correctly. The LSCB is aware of filtering policies and how these may differ between partner agencies.	All internet access for children through the LA is filtered by an accredited ISP and is monitored. All agencies within the LA have clear policies concerning requests for any changes to the filtering levels.	The internet service for children through the LA is provided by a fully accredited ISP. Accredited filtering is in place. The LA has provided enhanced user level filtering where appropriate. The LSCB receives monitoring reports from all member agencies and is able to use this data to inform their strategy. Evidence from monitoring and filtering logs shows that users have a mature approach and that there are very few incidents of misuse. The member agencies are 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 member agencies of the LSCB do not meet the e-safety technical requirements outlined in regional (eg SWGfL) and Local Authority Security Policies and Acceptable Usage Policies.	The member agencies meet the e-safety technical requirements outlined in regional (eg SWGfL) and Local Authority Security Policies and Acceptable Usage Policies.	The member agencies meet 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 ICT systems. The LSCB has an overview of any issues arising and ensures that appropriate action is taken.	The member agencies meet 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 ICT systems, with oversight from senior leaders. The LSCB has an overview of any issues arising, and this has an impact on policy and practice. The ICT infrastructure in all member agencies is secure and is not open to misuse or malicious attack.	The member agencies meet 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 ICT systems with oversight from senior leaders. The LSCB has an overview of any issues arising, and this has an impact on policy and practice. Internal reviews are augmented by rigorous external reviews of the security of school systems. Practice reflects up to date advancements in security, providing protection from new security threats as they arise.

What evidence could you use?

Filtering and monitoring policies

Logs and audits

Staff Handbooks

External inspections and reviews

Moving forward – the LSCB might wish to consider:
Are member organisations confident that their 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 internet filtering complemented by effective monitoring?

LSCB E-Safety Self Review Tool

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 within organisations and in the wider community.

ELEMENT B	Education and Training
STRAND 1	**E-Safety Training Strategy**

Aspect 1 — E-Safety Training Strategy

Level 5	Level 4	Level 3	Level 2	Level 1
There is no LSCB E-Safety Training Strategy.	An LSCB E-Safety Training Strategy is being developed.	An LSCB E-Safety Training Strategy is in place. An audit of e-safety training resources and a needs analysis have been carried out.	An LSCB E-Safety Training Strategy is in place. An audit of e-safety training resources and a needs analysis have been carried out. The strategy covers e-safety awareness training for all those who come into contact with children across member agencies.	An LSCB E-Safety Training Strategy is in place. An audit of e-safety training resources and a needs analysis have been carried out. The strategy covers e-safety awareness training for all those who come into contact with children across member agencies. The strategy gives consideration to ways of including awareness of e-safety in other training such as local child protection / safeguarding training.

STRAND 2	**Children and Yound People**

Aspect 1 — E-safety education

Level 5	Level 4	Level 3	Level 2	Level 1
There is no planned programme of e-safety education for member agencies of the LSCB.	A planned programme of e-safety education is being developed for some, but not all, member agencies of the LSCB.	A planned e-safety education programme takes place within schools. Pupils / students are aware of e-safety issues and are empowered to stay safe. Appropriate e-safety resources are used. The LSCB 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. The LSCB has identified those children who are not catered for by the mainstream school provision and is implementing other ways to raise awareness with them.	In addition to the e-safety education carried out in schools, other member agencies of the LSCB take an active role in providing awareness and education for children and young people around e-safety. As a result, children and young people are aware of e-safety issues and understand and follow the e-safety and acceptable use policies. Appropriate e-safety resources are used. The LSCB is effective in ensuring that member agencies provide the necessary education and protection of vulnerable children who may be put at particular risk from their and others' actions on-line. The LSCB regularly evaluates the effectiveness and impact of e-safety programmes.	In addition to the e-safety education carried out in schools, other member agencies of the LSCB take an active role in providing awareness and education for children and young people around e-safety. As a result, children and young people are aware of e-safety issues and understand and follow the e-safety and acceptable use policies. Appropriate e-safety resources are used. The LSCB is effective in ensuring that member agencies provide the necessary education and protection of vulnerable children who may be put at particular risk from their and others' actions on-line. The LSCB regularly evaluates the effectiveness and impact of e-safety programmes. All children and young people in the local authority have access to good quality e-safety education.

What evidence could you use?

Schemes of work

Training programmes

Educational / training resources

Website, newsletters, publicity materials

E-Safety Strategy

Staff training needs analysis

Moving forward – the LSCB might wish to consider:
Is e-safety education and training fully embedded in all member agencies? Does e-safety education and training help all users (staff and young people) to become informed and responsible users – both within and outside the member agencies? Do all levels of child protection training include an e-safety element?

LSCB E-Safety Self Review Tool

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 within organisations and in the wider community.

ELEMENT C	Education and Training				
STRAND 2	Children and Young People				

	Level 5	Level 4	Level 3	Level 2	Level 1
Aspect 2 **The contribution of children and young people**	The LCSB E-Safety Sub group does not acknowledge or use the high level of skills and knowledge of young people in the use of new technologies. The wishes and feelings of young people are not taken into account in the work of the E-Safety Sub group.	The LSCB E-Safety Sub group is developing opportunities to acknowledge and use the high level of skills and knowledge of young people in the use of new technologies. It is considering how the wishes and feelings of young people may be taken into account in the work of the E-Safety Sub group.	The LSCB E-Safety Sub group acknowledges, learns from and uses the high level of skills and knowledge of young people in the use of new technologies. There is youth representation on the E-Safety Sub group.	The LSCB E-Safety Sub group acknowledges, learns from and uses the high level of skills and knowledge of young people in the use of new technologies. The LSCB promotes the voice of young people on the E-Safety Sub-Group and they have had an active role in decisions about training for children and young people throughout the LA. Peer mentoring and other youth initiated activities are taking place with a range of member agencies.	The LSCB E-Safety Sub group acknowledges, learns from and uses the high level of skills and knowledge of young people in the use of new technologies. The LSCB promotes the voice of young people on the E-Safety Sub-Group and they have had an active role in decisions about training for children and young people throughout the LA. Peer mentoring and other youth initiated activities are taking place with a range of member agencies. Young people are involved in awareness raising with, and the training of, adults.

What evidence could you use?

Peer mentoring programmes

Buddying schemes

Contributions from children and young people in member agencies

Consultation reports

Moving forward – the LSCB might wish to consider:
Does the LSCB and its member agencies acknowledge and make full use of the contribution that young people as "digital natives" can make to e-safety?

LSCB E-Safety Self Review Tool

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 within organisations and in the wider community.

ELEMENT C	Education and Training				
STRAND 3	Staff				

Aspect 1
Staff training

Level 5	Level 4	Level 3	Level 2	Level 1
There is no formal e-safety training programme for staff in member agencies. Child Protection / Safeguarding training does not cover e-safety.	A formal e-safety staff training programme is being developed in member agencies. LSCB statutory multi-agency training on child protection / safeguarding has an e-safety element built into it.	A planned programme of formal e-safety training is made available to staff in member agencies. E-safety training is an integral part of Child Protection / Safeguarding training and vice versa. The LSCB E-Safety Sub group has carried out an audit of e-safety training needs. E-safety training is included in the induction programmes for new staff, but not in all member agencies. Staff responsible for managing the technical infrastructure receive relevant e-safety training and support.	There is a planned programme of formal staff e-safety training in member agencies. E-safety training is an integral part of Child Protection / Safeguarding training and vice versa. The LSCB E-Safety Sub group has carried out an audit of e-safety training needs. E-safety training is included in the induction programmes for all new staff, ensuring that they fully understand the relevant e-safety policies and Acceptable Use Policies that relate to their organisation. All relevant staff have an up to date awareness of e-safety matters, of the current LSCB e-safety policy and practices and are aware of child protection / safeguarding procedures. Staff responsible for managing the technical infrastructure receive relevant e-safety training and support.	There is a planned programme of formal staff e-safety training in all member agencies. E-safety training is an integral part of Child Protection / Safeguarding training and vice versa. The LSCB E-Safety Sub group has carried out an audit of e-safety training needs. E-safety training is included in the induction programmes for all new staff, ensuring that they fully understand the relevant e-safety policies and Acceptable Use Policies that relate to their organisation. All relevant staff have an up to date awareness of e-safety matters, of the current LSCB e-safety policy and practices and are aware of child protection / safeguarding procedures. The culture of member agencies ensures that staff support each other in sharing knowledge and good practice about e-safety. The LSCB and member agencies take every opportunity to research and understand good practice that is taking place elsewhere. Staff responsible for managing the technical infrastructure receive specific and high level e-safety training and support.

What evidence could you use?

Staff training needs analysis

Staff training programmes

CPD portfolios

Induction programmes

Good practice visits

Moving forward – the LSCB might wish to consider:
Do all staff, in all member agencies, 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?

LSCB E-Safety Self Review Tool

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 the organisation and in the wider community.

ELEMENT C	Education and Training

STRAND 4	Parents and Carers

	Level 5	Level 4	Level 3	Level 2	Level 1
Aspect 1 **Parental education (Parents, carers and wider family members)**	The LSCB and it's member agencies do not provide opportunities for parents and carers to receive education or information about e-safety.	The LSCB is coordinating and developing opportunities for parents and carers to receive education or information about e-safety.	The LSCB ensures that there is local provision for parents and carers to receive education or information about e-safety.	The LSCB, through the member agencies, provides opportunities for parents and other adults to receive e-safety training and awareness raising. These hands-on sessions can be accessed through a variety of means. Parents and carers know who to contact if they are worried about e-safety issues.	The LSC, through the member agencies, provides opportunities for parents and other adults to receive e-safety training and awareness raising. These hands-on sessions can be accessed through a variety of means. Parents and carers know who to contact if they are worried about e-safety issues. The LSCB and member agencies are effectively engaging "hard to reach" parents in e-safety programmes.

STRAND 5	Wider Community

	Level 5	Level 4	Level 3	Level 2	Level 1
Aspect 1 **Raising E-Safety Awareness**	The LSCB has not audited the level of e-safety awareness among member agencies and the wider community.	The LSCB is auditing the level of e-safety awareness among member agencies and the wider community. E-safety awareness is being developed among member agencies and the wider community.	The LSCB has developed and is implementing a strategy to raise levels of e-safety awareness among member agencies and the wider community.	The LSCB has developed and is implementing a strategy to raise levels of e-safety awareness among member agencies and the wider community. Issues are treated in a balanced way, alleviating fears, placing the risks within a context and promoting the positive use of technology.	The LSCB has developed and is implementing a strategy to raise levels of e-safety awareness among member agencies and the wider community. Issues are treated in a balanced way, alleviating fears, placing the risks within a context and promoting the positive use of technology. The LSCB and member agencies recognise the significant role that the community can play in raising e-safety awareness. Members of the community are involved, whenever possible, in the planning and delivery of awareness raising programmes.

What evidence could you use?

Acceptable Use Policies

Letters to parents and carers, newsletters, website

Parents / family evenings & courses

Family learning events

Attendance records for parents / family sessions

Moving forward – the LSCB might wish to consider:
Does the LSCB and member agencies acknowledge the importance of parents, carers and wider family members in e-safety education and the monitoring / regulation of the children's on-line experiences (particularly out of school)? Do they provide sufficient opportunities parents and carers to gain the information and support they need to allow them to carry out this role? Is this service also available to members of the community? Are member agencies involving "hard to reach" parents and carers?

LSCB E-Safety Self Review Tool

Element 4 of 4 This element reflects the importance of organisations knowing how the effectiveness of their policies and practice is impacting on e-safety outcomes. Have member agencies considered how they will monitor and is monitoring embedded in practice?

	ELEMENT D	Standards and Inspection				What evidence could you use?
	STRAND 4	Monitoring				
	Level 5	**Level 4**	**Level 3**	**Level 2**	**Level 1**	
Aspect 1 **Monitoring and Reporting of E-Safety Incidents**	There is no LSCB framework for the monitoring and reporting of e-safety incidents in member agencies.	Monitoring of e-safety incidents takes place in some, but not all member agencies. An LSCB monitoring and reporting framework is being developed.	There is an LSCB monitoring and reporting framework. Monitoring of e-safety incidents takes place in all member agencies, within a minimum dataset (as recommended in Becta guidance). The records are reviewed / audited and reported to the LSCB.	Monitoring and recording of e-safety incidents takes place in all member agencies, within a minimum dataset established in the LSCB monitoring and reporting framework. The records are regularly reviewed / audited and reported to the LSCB. Monitoring and reporting of incidents contributes to the development of LSCB e-safety policy and practice.	Monitoring and recording of e-safety incidents takes place in all member agencies, within a minimum dataset established in the LSCB monitoring and reporting framework. The records are regularly reviewed / audited and reported to the LSCB. Monitoring and reporting of incidents identifies emerging trends and contributes to the development of the LSCB e-safety strategy and to policy and practice in member agencies. As a result the LSCB is proactive in addressing e-safety issues.	Incident logs and audits / reviews Action / Development Plans Self Evaluations Minutes of meetings of relevant groups, and committees Monitoring reports External inspection / reviews Audits / stocktakes
Aspect 2 **Monitoring the impact of the e-safety strategy**	There is no monitoring of the impact of the LSCB e-safety strategy.	Monitoring of the impact of the LSCB e-safety strategy is being developed.	The impact of the LSCB e-safety strategy is monitored through the review / audit of e-safety incident logs and surveys of staff, young people and parents / carers.	The impact of the LSCB e-safety strategy is monitored through the review / audit of e-safety incident logs and surveys of staff, young people and parents / carers. There is balanced professional debate about the evidence taken from the review / audit of the e-safety incident logs and the peer-review process based on self evaluation.	The impact of the LSCB e-safety strategy is monitored through the review / audit of e-safety incident logs and surveys of staff, young people and parents / carers. There is balanced professional debate about the evidence taken from the review / audit of the e-safety incident logs and the peer-review process based on self evaluation. All member agencies are committed to this process and collectively share issues and good practice, in order to contribute to the development of policies and practice across the local area.	

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

LSCB E-Safety Self Review Tool

R1

Record Sheet 1 This record sheet should be used with the SWGfL LSCB E-Safety Self Review Tool. LSCBs should indicate in the Level columns which level best illustrates their current position on the framework. Comments and evidence sources may be added as relevant.

360 degree safe LSCB E-Safety Self Review Tool

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 Sub Group							
Aspect 2 E-Safety responsibilities							
Aspect 3 The LSCB							

STRAND 2	Policies

	Level 5	Level 4	Level 3	Level 2	Level 1	Comment	Sources of Evidence
Aspect 1 Strategic development							
Aspect 2 E-Safety Policies							
Aspect 3 Programme of Work (Action Plan)							
Aspect 4 Acceptable Use Policies							
Aspect 5 Embedding Policy and Practice							
Aspect 6 Reporting (in member agencies)							
Aspect 7 Dealing with e-safety incidents/sanctions							

LSCB E-Safety Self Review Tool

Record Sheet 2

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

ELEMENT A — Policy and Leadership

STRAND 3 — Communication and Communications Technologies

	Level 5	Level 4	Level 3	Level 2	Level 1	Comment	Sources of Evidence
Aspect 1 Communications technologies							
Aspect 2 LSCB E-Safety Communications Plan							
Aspect 3 Awareness Raising							
Aspect 4 Media Strategy							
Aspect 5 Professional standards							

ELEMENT B — Infracture

STRAND 1 — Services

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

ELEMENT C — Education

STRAND 1 — E-Safety Training Strategy

	Level 5	Level 4	Level 3	Level 2	Level 1	Comment	Sources of Evidence
Aspect 1 E-Safety Training Strategy							

LSCB E-Safety Self Review Tool

R3

Record Sheet 3 — This record sheet should be used with the SWGfL LSCB E-Safety Self Review Tool. LSCBs should indicate in the Level columns which level best illustrates their current position on the framework. Comments and evidence sources may be added as relevant.

ELEMENT C — **Education**

STRAND 2 — **Children and Young People**

	Level 5	Level 4	Level 3	Level 2	Level 1	Comment	Sources of Evidence
Aspect 1 E-Safety Education							
Aspect 2 The contribution of children and young people							

STRAND 3 — **Staff**

	Level 5	Level 4	Level 3	Level 2	Level 1	Comment	Sources of Evidence
Aspect 1 Staff training							

STRAND 4 — **Parents and Carers**

	Level 5	Level 4	Level 3	Level 2	Level 1	Comment	Sources of Evidence
Aspect 1 Parental education							

STRAND 5 — **Wider Community**

	Level 5	Level 4	Level 3	Level 2	Level 1	Comment	Sources of Evidence
Aspect 1 Community understanding							

LSCB E-Safety Self Review Tool

R4

Record Sheet 4

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

ELEMENT D — Standards and Inspection

STRAND 1 — Monitoring

	Level 5	Level 4	Level 3	Level 2	Level 1	Comment	Sources of Evidence
Aspect 1 Monitoring and Reporting of E-Safety Incidents							
Aspect 2 Monitoring the impact of the e-safety strategy							

Name of LSCB	
Contact Person	
Address	
Email Address	
Telephone Number	

© SWGfL 2010