Teeswide Local Safeguarding Children Boards

eSafety Standards self audit tool

Technology has transformed learning and communication for individuals and for all organisations that work with people. However, the use of technology can also bring risks. Organisations that work with people must be aware of these risks and must have good policies and procedures in place to ensure the online safety of users, while making the most of online opportunities.

Across Tees the Local Safeguarding Children Boards (LSCB) are introducing minimum standards of safety for using digital technology, whilst still allowing maximum access to learning, and stressing the importance of using of modern sites such as facebook, twitter, You Tube, MSN and the like. These standards will:

- Show why eSafety is important and should involve everyone.
- Helps you to create a safer online environment for the people in your care.
- Provides guidance and resources
- Provides a way of identifying strengths and weaknesses
- Provides a way to move from a basic level of eSafety to best practice

Any organisation turning off a social networking, blogging or video site or by blocking access to such sites will not be supporting the education of users in their safe and proper use. These sites, when used safely and properly, are extremely useful tools that are regularly used.

Instead, the Tees LSCB's strongly believes that the process of education in their use is preferable to the blocking of them. All of the standards that are included within this document are inline with current Ofsted guidelines.

How to use the Standards self audit tool

The standards are divided into three sections, and each section includes a number of parts.

Each part has three levels:

RED There is little or no online safety policy and practice in place.

AMBER Basic online safety policy and practice is in place.

GREEN Online safety policy and practice is clear, agreed and respected

A record sheet is attached for organisations to record their level for each part with space to add comments. The sources of evidence column will help organisations show how they have achieved the level they are at.

Teeswide Local Safeguarding Children Boards eSafety Standards self audit tool

Management: This section reflects the importance of having effective leadership; clear policies that are agreed, understood and respected by everyone and regularly reviewed. There is good practice in keeping data safe.

	Standard	Red	Amber	Green	Evidence to be used
Leadership	Is there a designated person who has responsibility for managing the safety of all users and for ensuring all software is fully licensed for use?	No one has overall responsibility for managing the safety of all users	A designated person oversees the management of the safety of all users.	A designated person oversees the management of all users and ensures it is agreed and respected by all.	Organisation vision, aims or mission statement Development Plan Structure Chart Internal review documents Job descriptions Policy documents eg. Acceptable Use Policies / Online Safety / E-Safety Policies / Data Security Minutes of meetings of relevant groups and committees Incident logs and monitoring reports
Policy	Are there policies and guidelines in place and does everyone understand them? Policies must include bullying and particularly cyber bullying	There are no policies or guidelines in place for managing the safety of users	There is an acceptable use policy in place.	There is a clear agreed and respected eSafety policy in place, supported by an agreed Acceptable use Policy. Integrated into the organisation's safeguarding policies.	
Reviewing practice	How do you know your practices help safeguard users on line?	There are no regular checks	Some aspects of eSafety have been checked, but need further improvement.	There are regular checks which lead to improvements that have an impact on safeguarding users.	
Data Security	How safe is the personal data you use and keep?	There are very few measures in place to protect personal data	There are basic measures in place to protect personal data and these meet legal requirements.	The required personal data security measures are in place and understood by all users. This ensures the safe keeping of personal data, minimising the risk of loss or misuse.	

People: This section reflects the importance of effective eSafety education and training for everyone. Users should know how to report incidents and should understand the sanctions.

	Standard	Red	Amber	Green	Evidence to be used
Reporting	Is it clear how to report eSafety issues including access to inappropriate material?	There is no reporting process.	A reporting process is in place.	A reporting process is in place and is widely used, acted upon and recorded.	Reporting and sanctions policies Incident logs and monitoring reports Online safety / e-safety awareness programmes Online safety/ e-safety resources Induction policies and procedures Training programmes Curriculum Planning Online Safety Resources
Sanctions	Are people aware of the consequences of their actions?	There are no consistent sanctions for the misuse of digital technologies.	Sanctions are in place for misuse of digital technologies.	All users understand and respect the sanctions for the misuse of digital technologies. Positive online behaviour is recognised and rewarded.	
Education	How do you ensure people are made aware of how to stay safe online?	There is no provision to make people aware of eSafety. .	There is some provision to make users aware of eSafety but this is neither consistent nor planned.	There is consistent, planned and apt provision ensuring awareness of eSafety. Trained delivery of programmes may be by teachers, external agencies and peers	
Training	How do you ensure that staff and volunteers follow best practice when using digital technologies?	There is no planned programme of eSafety training for staff and/or volunteers.	eSafety training is available for some staff and/or volunteers but is neither consistent, nor planned.	There is a planned compulsory programme of eSafety training for all staff and/or volunteers with induction and regular updates that supports safeguarding practice. Some staff and/or volunteers have opportunities to achieve relevant accreditation	

Technology: This section reflects the importance of having effective systems in place to ensure the security of devices, systems, images, personal devices and data. It should be regularly reviewed and updated, in the light of constantly changing technology and new online security threats.

	Standard	Red	Amber	Green	Evidence to be used
Communications	Do all users communicate safely and appropriately when using online technologies eg email, messaging, websites and learning environments?	Users are unclear about how they should communicate safely and appropriately when using online technologies.	Users have been informed about safe and appropriate use of current digital technologies. Staff and volunteers understand that communications with young people and their families should be professional in nature.	There is agreed communication strategy that is respected by all. It specifies safe and appropriate use of current digital technologies. Communications are carried out on the organisation's "official systems" and are monitored.	Communications strategy / policy Staff handbook Policy / guidance for staff / volunteers working with young people Website / publications Digital images / video policy Policies covering personal devices eg mobile phones ICT security policies Password policy Filtering policy Monitoring logs Incident logs with evidence of monitoring and auditing
Personal Devices	Do you encourage the safe use of personal devices such as mobile phones, hand held devices, gaming consoles etc	Safeguarding issues around the use of personal devices have not been addressed.	The risks and benefits of the using personal devices have been considered and there is some guidance to encourage safe use.	The safe use of personal devices is encouraged and respected by everyone. Their use is regularly reviewed in the light of emerging new technologies	
Digital Images and Video	Do you minimise risks involved in taking, storing, using, sharing,publishing and distributing digital images and video?	There is no clear practice relating to the management of digital images and video.	There is some awareness of issues relating to digital images and video but practice is not well established or consistent.	There is clear guidance with regards digital images and video which meets expected standards. There are well established procedures for obtaining (parental) permission. These standards are rigorously applied by all users and are reviewed regularly.	

Devices	Are the devices you use protected from viruses, hacking etc. Are they regularly updated and password protected?	Devices are not protected, nor regularly updated. Passwords are not used.	Some devices have anti virus and Internet security software but this is not well managed. Passwords are used.	Devices are regularly updated and protected against threats. All users have individual passwords that are strong and regularly updated.	
Internet access	Is there safe access to the internet? Is the access filtered or monitored and supervisied?	A lack of filtering or supervision means that safe access to the internet cannot be guaranteed.	Access to the internet is monitored or filtered (or both),generally supervised with staff being aware of policy.	An accredited or approved ISP is used to provide internet access or there is an effective local filtering system combined with consistent supervision. Forensic software is provided to promote safe use of internet, and includes the facility to protect from bullying, harassment and harm.	
Monitoring of Network and devices	How do you know what your devices and systems are used for?	No monitoring takes place.	Some monitoring takes place but is not carried out to a planned programme and therefore may not give a clear and accurate picture.	Staff are aware that monitoring of system use is in place, is recorded and regularly checked. Any issues identified are acted on in conjunction with policy and procedures including relevant sanctions and rewards.	

Teeswide Local Safeguarding Children Boards

eSafety Standards self audit tool record sheet 1:

Name of Organisation:	
Type of Organisation:	
Contact Person:	
Organisation Address:	
Email Address:	
Telephone Number:	

Teeswide Local Safeguarding Children Boards

eSafety Standards self audit tool record sheets 2:

Management					
	Red	**Amber**	**Green**	**Comment**	**Evidence Used**
Leadership					
Policy					
Reviewing Practice					
Data Security					

People					
	Red	**Amber**	**Green**	**Comment**	**Evidence Used**
Reporting					
Sanctions					
Education					
Training					

Technology					
	Red	**Amber**	**Green**	**Comment**	**Evidence Used**
Communications					
Personal Devices					
Digital Images and Video					
Devices					
Filtering and Supervising					
Monitoring					

Appendix 1

<u>Any Acceptable Use Policy (AUP) will include the following:</u>

Procedures must be in place to ensure the storing, distributing, transmitting or permitting the storage, distribution or transmission (whether intentionally or otherwise) of any unlawful material or of any material which falls into the categories mentioned below through the Service is prohibited:

- in violation of any law or regulation
- which is defamatory, offensive, abusive, indecent, obscene
- which is violent
- which constitutes harassment
- is in breach of confidence, privacy, trade secrets
- is in breach of any third party Intellectual Property rights (including copyright)
- is in breach of any other rights or has any fraudulent purpose or effect.
- is in breach of fraud or any criminal activity legislation

Violations may include, but are not limited to, the following:

- Unauthorised access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network

- Unauthorised monitoring of data or traffic on any network or system without express authorisation of the owner of the system or network
- Interfering with any user, host or network including mailbombing, flooding, and deliberate attempts to overload a system and broadcast attacks.

Any broadband service must comply with banned sites listed by the Internet Watch Foundation. Attempts to access these illegal banned sites will result in the user being reported to the appropriate police authorities resulting in legal or civil actions.

Laws regulating such diverse subjects as intellectual property, fraud, defamation, pornography, insurance, banking, financial services and tax, apply equally to on-line activities. Documents must not be published or accessed on the web which are defamatory or which may constitute intimidating, hostile or offensive material on the basis of sex, race, colour, religion, national origin, sexual orientation or disability.

Organisations must ensure all of its users are aware of how to report suspicious activity they detect e.g. to the law enforcement agency CEOP (Child Exploitation and Online Protection Centre) or the hotline for reporting illegal online content the Internet Watch Foundation (IWF)

Individual will not send e-mails to any user who does not wish to receive it when a request to stop has been received, or is:

- in violation of any law or regulation
- which is defamatory, offensive, abusive, indecent, obscene, violent, or constitutes harassment
- is in breach of confidence, privacy, trade secrets, any third party Intellectual Property rights (including copyright)
- is in breach of any other rights or has any fraudulent purpose or any criminal activity legislation
- Chain letters are unsolicited by definition and will not be sent.
- Flood emails will result in the site's broadband connection being shutdown
- Organisations will not send, distribute, or reply to mailbombs, (the e-mailing of a single message to many users, or the emailing of large or multiple files or messages to a single user with malicious intent.)
- Organisations will not use false, or alter email headers to conceal their e-mail address or to prevent Internet users from responding to messages. You must not use any email address that you are not authorised to use.
- Organisations will not operate, host, provide hosting facilities to or assist in anyway whatsoever any web site, email address, email service, file transfer protocol (FTP) service or any other online service, which is advertised or promoted by means of Unsolicited Bulk Email.