Euxton CE Primary School online safety policy

Contents

Online Safety Policy – Euxton CE Primary School

1. Introduction

This policy applies to all members of Euxton CE Primary School's community (including staff, pupils, parents/carers, governors, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our online safety policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings. The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection.

2. Euxton CE Primary School's Vision for online safety

Euxton CE Primary School aims to embrace modern technology to its fullest potential, and promote its safe use by all members of the Euxton CE Primary School's community. We want all our children and staff to be confident with a range of technology, using it confidently to meet our needs. We believe whole-heartedly that children at Euxton CE Primary School should be educated thoroughly in keeping safe when using ICT, from their very first days at the school. As a result, our children will be safe in using technology they may encounter both within, and out of, the school environment.

Our children will leave Euxton CE Primary School knowing how to use technology effectively, responsibly and safely, and will be equipped with the skills they will need to be successful in the rest of their lives.

3. The role of the school's online safety champion

Our Online Safety Champion is the Computing Coordinator.

The role of the Online Safety Champion in our school includes:

- promoting and monitoring the safe use of ICT within school

- ensuring all children are educated in the safe use of ICT, within and out of the school environment

- monitoring and reviewing the Online Safety Policy, and Acceptable Use Policies

- keeping up-to-date with technological and online safety developments

- training staff members on the safe use of technology as necessary, ensuring all staff are aware of reporting procedures in the event of an online safety incident occurring.

- being the school's point of contact for online safety related issues and incidents

- liaising with the school's DSP where necessary in the case of child protection

- ensuring the online safety Incident Log is appropriately maintained and regularly reviewed

- arranging or providing online safety advice/training for parents/carers/governors as necessary

4. Policies and practices

This section of the Online Safety Policy sets out our school's approach to online safety along with the various procedures to be followed in the event of an incident.

This Online Safety Policy should be read in conjunction with the following other related policies and documents:

ICT Acceptable Use Policy

Computing Policy

Safeguarding Policy

Data Protection Policy

PSHE Policy

Staff Handbook

Induction Policy

Job Descriptions

4.1 Security and data management

In line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection

In our school, data is kept secure and all staff are informed as to what they can/cannot do with regard to data in the following ways:

1. The Head teacher has ultimate responsibility for all the information that is held in school, and is in charge of managing all data and information, both within and outside the school environment.

2. Relevant staff will be shown the location of data necessary to their position during the induction process.

3. All staff with access to personal data are made aware of their legal responsibilities as part of the induction process.

4. Staff should only access data with which they are authorised to do in line with their job description.

5. Sensitive and confidential information is kept securely, protected by passwords where necessary. Computers with access to sensitive and confidential information should not be left logged on, unless the room itself is secure.

6. Staff with access to school data outside of the school environment are made aware of the importance of ensuring the security of the data, for example ensuring laptop computers and wireless networks are password-protected. Further guidance is provided in the Data Protection Policy, and the Staff Handbook. Staff should only access data outside of the school environment where it is necessary to fulfil their job description, and where the school premises are closed.

7. All data is backed up daily, in order to reduce the risk of data loss.

4.2 Use of mobile devices

In our school we recognise the use of mobile devices offers a range of opportunities to extend children's learning. However, the following statements must be considered when using these devices:

1. All devices with 3G/4G wireless connections can access unfiltered internet content. Therefore, this facility must be turned off before children use such devices.

2. Any devices that use the school network must contain up-to-date virus software.

3. Portable USB devices are permitted to be used, as the school has up-to-date Anti-Virus software. However, staff must ensure that personal computers that the devices are also used with have sufficient Anti-Virus protection.

4. Staff are permitted to bring in personal mobile devices, however these must be kept securely. These must only be used appropriately for personal reasons, for example not making or receiving personal phone calls when children are present. In addition, phones should only be used by staff outside working hours, except when absolutely necessary. Any data captured on such devices for professional reasons, for example a voice recording during a lesson, must be transferred onto a school computer and deleted immediately from the mobile device. It is not acceptable for staff to take pictures on mobile phones.

5. Pupils must not bring a mobile phone into school without permission from home and school. Mobile phones which have been allowed will be kept securely in the office. Teachers may confiscate any personal mobile devices which children bring into school without permission, and will arrange for them to be kept securely in the office.

4.3 Use of digital media

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below:

1. All children, on induction to the school, are required to consent to the use of photographs, videos and appearance in local (or national) media. An up-to-date list of permissions is kept in the school office, where staff can access them prior to taking any pictures and videos. A child's parents/carers can change these permissions at any time by notifying the school office, where a new form will need to be completed and signed.

2. Images and videos may be retained and used by the school, for example in promotional literature, for a maximum period of 5 years after the child has left the school. This is made clear on the consent form signed on induction to the school.

3. Full names or personal details will not be used on any digital media that is published.

4. Parents/Carers are not permitted to video or photograph certain school events, such as shows, although separate opportunities to take photographs are made available. Events may be recorded by the school, or by a private company assigned by the school, and later made available for parents/carers to purchase.
Parents/Carers are reminded of this before each event. Parents/Carers who do not wish their child to be photographed/recorded can express these wishes to the Head teacher or other staff, who will make appropriate arrangements.

5. Staff are trained to understand the risks associated with publishing images, particularly in relation to the use of personal Social Network sites. Further details are available in the Acceptable Use Policy for staff use of the internet.

6. Photographs/videos should only be taken using school equipment, for school purposes. This content should only be stored on equipment that is for predominantly school use. Staff should always make sure that children are appropriately dressed and not participating in activities that could be misinterpreted.

7. All staff, parents/carers, and pupils are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites without the consent of the persons involved. This is achieved through training, information evenings, lesson time, literature and a dedicated website area.

8. The guidelines for safe practice and relevant Acceptable Use Policies are monitored every year by the online safety champion, who will liaise with the Headteacher as required.

4.4 Communication technologies

Email:

In our school the following statements reflect our practice in the use of email:

1. It is recommended that all users have access to the Lancashire's preferred school e-mail system Microsoft Office 365 (Email and Office Cloud Applications). Any staff wishing to have a school email

address should request that one is created by the Headteacher.

2. Lancashire's preferred school e-mail system Microsoft Office 365's filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to the Headteacher.

3. All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school. Personal email accounts should not be checked in the presence of children, or connected to the overhead projectors/whiteboards.

4. All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.

5. All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.

6. All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

7. Children are not permitted to access personal email accounts in the school environment.

Social Networks:

Social Network sites allow users to be part of an online community. Current popular examples of these are Facebook, Twitter and Club Penguin. These sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user.

As a user on a Social Network site, you may have access to view other users' content, send messages and leave comments. NB: Many Social Network sites have age restrictions for membership e.g. Facebook minimum age is 13 years old.

In our school the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:

1. Staff must not give personal contact details to pupils or parents/carers including mobile telephone numbers, or details of any blogs or personal websites.

2. Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.

3. If a Social Network site is used by staff, details must not be shared with pupils and privacy settings be set at maximum. Staff should be aware that 'friends of friends' may be able to view 'tagged' photographs/comments, which may bring the individual member of staff or the school into disrepute. Comments made and photographs posted reflect the professional reputation of the school, and once posted cannot be un-done.

4. Pupils must never be added as 'friends' by staff. If a pupil persists in making friend requests, it is necessary to log the incident in the online safety log and report to the online safety champion, who will deal with the matter appropriately.

5. No pupils under the age of 13 should be using Facebook. However, it is known that a large

proportion of children under this age do use this Social Network. It is the school's responsibility to ensure that children are educated on the safe use of all Social Networks, with particular attention to Facebook.

6. As part of our educating process, all children at Euxton CE Primary School will participate in 'Safer Internet Day' held each February.

Web sites and other online publications

At Euxton CE Primary School, the following statements outline what we consider to be acceptable and unacceptable use of websites and other online publications:

1. The school website will be maintained by the teaching staff and the IT Technician.

2. Content of the website will updated by all teachers and the headteacher.

3. The website is a fundamental place for communicating online safety messages to pupils and parents/carers, and has a dedicated online safety section.

4. All staff are aware of the guidance for the use of digital media and personal information on the website.

5. Any material for the website is passed to the Computing Coordinator, who updates the website periodically, ensuring relevant guidance is adhered to.

6. All materials on the website shall adhere to copyright restrictions.

7. Sensitive documents should only be available in 'read-only' formats, such as PDFs.

Video conferencing e.g. Skype:

On occasion, a class may wish to use video conferencing, for example to communicate with a partner school via Skype.

In our school the following statements outline what we consider to be acceptable and unacceptable use of Video conferencing:

1. Approval must be sought in advance from the Headteacher prior to video-conferencing taking place.

2. Only secure, approved programs to be used for video conferencing.

3. All pupils will be supervised when using video conferencing.

4. It should be made clear to the receiver that no recordings may be taken without permission.

5. Staff know how to terminate the video conference at any time.

4.5 Acceptable Use Policy (AUP)

An Acceptable Use Policy is intended to ensure that all users of technology within school will be responsible and stay safe. It ensures that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.

AUPs are recommended for Staff, Pupils, Governors and Visitors/Guests and must be signed and adhered to by users before access to technology is allowed. This agreement is a partnership between parents/carers, pupils and the school to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology must be kept in school and made available to all staff.

The school has the following AUP's in place (see appendices):

ICT AUP – Staff and Governor Agreement

ICT AUP – Supply Teacher and Visitors/Guests Agreement

ICT AUP – Pupils Agreement/online safety Rules

ICT AUP – Parent's letter

Euxton CE Primary School advocates and teaches the 'Think then Click' philosophy, and embeds Golden Rules for Staying Safe with ICT in teaching. These are displayed wherever computers are used in school.

4.6 Dealing with incidents

In the event that an online safety incident occurs, that contravenes the Online Safety Policy or agreed AUP's, it is important the protocol below will be followed. It is important to distinguish between illegal and inappropriate use of ICT. All incidents will be logged in the incident log kept by the Online Safety Champion.

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Head teacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). **Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence.** It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident (See Appendix). Always report potential illegal content to the Internet Watch Foundation (http://www.iwf.org.uk) .They are licensed to investigate – schools are not.
Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

More details regarding these categories can be found on the IWF website - http://www.iwf.org.uk.

Inappropriate use and sanctions

It is important that any incidents are dealt with quickly and actions are proportionate to the offence. If the guidelines or AUPs are breached, or suspected of being breached, the Headteacher should be notified if appropriate. Some examples of inappropriate incidents are listed below with possible sanctions, although this will ultimately be at the discretion of the Headteacher. All incidents should be logged in the online safety incident log.

Incident	Procedure and Sanctions
Accidental access to inappropriate materials.	• Minimise the webpage/turn the monitor off/click the 'Hector Protector' button. • Tell a trusted adult. • Enter the details in the Incident Log and report to LGfL filtering services if necessary. • Persistent 'accidental' offenders may need further disciplinary action.
Using other people's logins and passwords maliciously.	• Inform SLT or designated eSafety Champion. • Enter the details in the Incident Log. • Additional awareness raising of eSafety issues and the AUP with individual child/class. • More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. • Consider parent/carer involvement.
Deliberate searching for inappropriate materials.	
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate way.	

Where staff are suspected of contravening the AUP, this should be reported to the Headteacher who will take appropriate steps in accordance with the school's discipline policy.

Euxton CE Primary School uses a holistic approach to online safety, and as such all staff are responsible for dealing with online safety incidents appropriately at class level. The online safety champion should be notified of any online safety incidents, who will then liaise with the Headteacher as appropriate.

The online safety log book will be kept securely by the Online Safety Champion. This will be monitored regularly, with action plans put in place as necessary to avoid further incidents where possible.

The 'Lancashire online safety Incident/Escalation Procedures' document will be followed (see Appendix) as a framework for responding to incidents.

5. Infrastructure and technology

Euxton CE Primary School aims to ensure that our infrastructure and network is as safe and secure as possible. This section of the policy defines the policies and procedures in place to safeguard users.

The ICT network at Euxton CE Primary School is protected by the BT Lancashire Lightspeed filter. However, should unsuitable content not be detected by this filter, children are educated to minimise the screen and inform an adult immediately. Staff will subsequently report the URL of inappropriate content to BT Lancashire Lightspeed.

Sophos Anti-Virus is used by the school to protect the network and data from viruses, Trojans and Malware. The network is also protected by a Firewall.

Pupil Access:

Children should only access the internet using school computers when supervised by a trusted adult.

Passwords:

Staff passwords must contain a mixture of alphanumeric characters, and a mixture of uppercase and lower case letters. These must not be shared. Only staff user profiles will be able to make administrative changes to programmes and access the teachers' area of the network.

Pupils simply have to click log-on to their year of intake to access the school network; the password is the same as the year of intake. These profiles have limited privileges as designated by the teachers and IT technician.

The administrator's password for the overall network is available to the Headteacher, Computing Coordinator and IT Technician.

Software/hardware:

All software used in school must be owned by the school, or by staff at the school, with appropriate user licenses used.

Licenses should be kept centrally in the designated License folder, which is kept in the ICT suite. Where appropriate, any annual subscriptions should be renewed in good time. This is the

responsibility of the Computing Coordinator and Bursar/School Administrative Officer.

All ICT equipment and software is audited every 2 years at the same time as the ICT policy is reviewed. Any additional equipment required will be budgeted for in the annual Action Plan.

Software is installed on systems by Simon Walters, however all school staff are permitted to install necessary software providing they own the appropriate license for this. A copy of this should be entered into the License folder.

Managing the network and technical support:

The school network is managed by the IT Technician, who is responsible for all aspects of network technical support and maintenance. The IT Technician visits the school once a week to perform maintenance and solve any issues.

The following procedures are to be followed to ensure the network and all data remains secure:

- Servers, wireless systems and cabling are securely located and physical access restricted
- Wireless devices must have security enabled
- The wireless network is accessible only through a secure password, available only to the IT Technician, the Computing Coordinator and the Headteacher.
- The IT Technician is responsible for managing the security of the school network.
- The safety and security of the network is reviewed by the IT Technician on each maintenance visit.
- The IT Technician ensures that all computers are configured to receive all necessary updates and patches.
- There is a separate password for pupils and staff, who each have their own user profile. Only staff will have permissions to change their system profile and install necessary software. The pupils' profile will be reset when the user logs out, with any work saved to a separate hard disk. The overall network administrator password is available only to the IT Technician, the Computing Coordinator and the Headteacher.
- Staff and pupils must log out of computers and shut them down at the end of each session.
- If any users suspect a breach of network security, they should inform the Computing Coordinator immediately. The Computing Coordinator will then contact the IT Technician for assistance.
- Removable storage devices are permitted to be used in school, however if they contain any sensitive data they must be in password-protected, encrypted folders.
- Where school laptops are loaned to teachers, these may be used for acceptable personal use only. Further guidance can be found in the 'Staff Use of Internet' AUP.
- If network monitoring takes place, is it in accordance with the Data Protection Act (1998)?
- The Computing Coordinator and Headteacher are responsible for liaising with and managing the technical support staff from the IT Technician when using school computers. Logs are

kept each visit to ensure essential maintenance has taken place.

Filtering and virus protection:

Sophos Anti-Virus software is used on all school computers. This is updated regularly automatically by Simon Walters.

Any laptops or other devices that access the network must have up-to-date Anti-Virus software. The update configurations should be checked by the IT Technician whenever a new computer or device is used on the network. Staff are also responsible for making sure their particular system's Anti-Virus software is up-to-date, and are trained on how to do this.

6. Education and Training

Education and training are essential components of effective online safety provision. Equipping individuals, particularly pupils, with the appropriate skills and abilities to recognise the risks and how to deal with them is fundamental. Online safety is embedded within the curriculum and advantage taken of new opportunities to promote online safety. Pupils are taught online safety at the start of every new academic year in the autumn term and also throughout the year at the discretion of each class teacher.

6.1 Online Safety across the curriculum

Online safety is embedded in all ICT curriculum areas. The school also participates in the annual 'Safer Internet Day' every February, with specific teaching and discussion of online safety issues. Other issues such as online bullying is discussed in PSHE sessions.

All classes begin each academic year with a session reminding them of our school's online safety code. Where necessary, class teachers will differentiate their teaching to ensure all pupils remain safe when using technology.

Pupils are also reminded of relevant legislation regarding the internet, such as copyright implications.

Pupils are taught during online research lessons to critically evaluate materials and content. This is reinforced in all other cross-curricular ICT sessions.

Online safety rules are displayed wherever computers are used in school. This is differentiated by key stage.

6.2 Online Safety – Raising staff awareness

All staff, upon starting work at the school, are required to agree to the school's AUP and are provided with a copy of the Online Safety Policy and key staff guidelines, which includes personal safeguarding. Staff training updates for online safety will be delivered as necessary, with a minimum of once per academic year. All training and advice will be delivered by the Computing Coordinator. The Computing Coordinator/online safety Champion is aware of updates to online safety guidelines and receive external training as necessary.

All staff are expected to promote and model responsible use of ICT at all times, and all staff are responsible for promoting online safety whilst using ICT

6.3 Online Safety – Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).

Euxton CE Primary School offers regular opportunities for parents/carers and the wider community to be informed about online safety, including the benefits and risks of using various technologies. This takes place through:

- School newsletters.
- A dedicated area on the school website, which promotes external online safety resources and online materials.
- Joint online safety meetings held with St Mary's Catholic Primary School.

6.4 Online safety – Raising Governors' awareness

Governors are kept updated on arising online safety matters through the Annual Report to Governors. Governors also review and agree the Online Safety Policy annually, following discussion with the online safety Champion.

The online safety log book is also available to the Governors at any time and is kept in the staff room.

7 Standards and inspection

It is crucial that safeguarding procedures, including ICT, are monitored regularly to ensure that the policy is having the desired effect. It is the overall responsibility of the online safety Champion to ensure that the policy is effective in maintaining the safe use of ICT at Euxton CE Primary School.

The Online Safety Champion will:

- ensure a log book is in place for online safety incidents, which is monitored constantly and appropriate action taken. Additionally, the incident log will be reviewed at the same time as the online safety and ICT Policy, to ensure that any issues are addressed in changes to the policies.

- Any new technologies are risk assessed by the Online Safety Champion and all teachers, and Acceptable Use Policies amended/devised if necessary.

- Ensure that staff, parents/carers, pupils and Governors are informed of changes to policy and practice

- Review AUPs at least every 2 years, and more frequently as necessary should matters arise.

Overall, online safety at Euxton CE Primary School is the responsibility of all stakeholders – teachers, support staff, pupils, parents/carers and governors. It is vital that new technologies are readily embraced, with the appropriate steps taken to ensure that they are always used safely.

Euxton CE Primary School online safety policy

Written by Lee Price November 2014

Updated by Lee Price June 2017

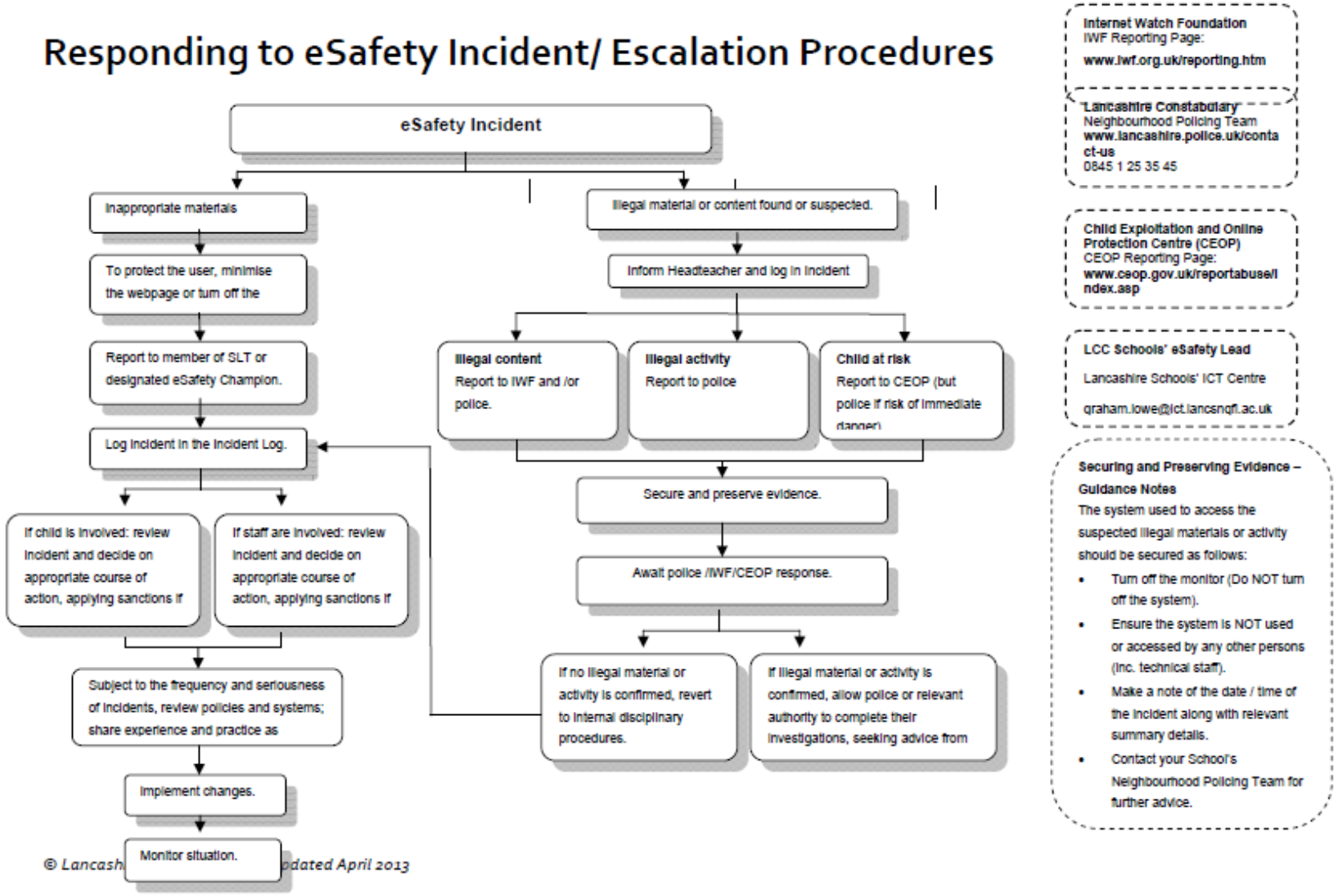
Reviewed and approved by the Governing Body June 2017

Online Safety Incident Log

All online safety incidents must be recorded by the member of staff who teaches and/or witness' the incident. The school Online Safety Champion keeps the log and the Heateacher must also be informed.

This incident log will be monitored and reviewed regularly by the Headteacher and Chair of Governors.

Date / Time of Incident	Type of Incident	Name of pupil/s and staff involved	System details	Incident details	Resulting actions taken and by whom (and signed)
01 Jan 2010 9.50 am	Accessing Inappropriate Website	A N Other (Pupil) A N Staff (Class Teacher)	Class 1 Computer 1.5	Pupil observed by Class Teacher deliberately attempting to access adult websites.	Pupil referred to Headteacher and given warning in line with sanctions policy for 1st time infringement of AUP. Site reported to LGFL as inappropriate.


Responding to eSafety Incident/ Escalation Procedures
eSafety Incident
Inappropriate materials
To protect the user, minimise the webpage or turn off the
Report to member of SLT or designated eSafety Champion.
Log incident in the Incident Log.
If child is involved: review incident and decide on appropriate course of action, applying sanctions if
If staff are involved: review incident and decide on appropriate course of action, applying sanctions if
Subject to the frequency and seriousness of incidents, review policies and systems; share experience and practice as
Implement changes.
Monitor situation.
Illegal material or content found or suspected.
Inform Headteacher and log in incident
Illegal content
Report to IWF and /or police.
Illegal activity
Report to police
Child at risk
Report to CEOP (but police if risk of immediate
Secure and preserve evidence.
Await police /IWF/CEOP response.
If no illegal material or activity is confirmed, revert to internal disciplinary procedures.
If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking advice from
Internet Watch Foundation
IWF Reporting Page:
www.iwf.org.uk/reporting.htm
Lancashire Constabulary
Neighbourhood Policing Team
www.lancashire.police.uk/contact-us
0845 1 25 35 45
Child Exploitation and Online Protection Centre (CEOP)
CEOP Reporting Page:
www.ceop.gov.uk/reportabuse/index.asp
LCC Schools' eSafety Lead
Lancashire Schools' ICT Centre
graham.lowe@ict.lancsngfl.ac.uk
Securing and Preserving Evidence – Guidance Notes
The system used to access the suspected illegal materials or activity should be secured as follows:
Turn off the monitor (Do NOT turn off the system).
Ensure the system is NOT used or accessed by any other persons (inc. technical staff).
Make a note of the date / time of the incident along with relevant summary details.
Contact your School's Neighbourhood Policing Team for further advice.
© Lancash
odated April 2013