Primary eSafety

Updated April 2013

Guidance Document

Lancashire County Council

www.lancashire.gov.uk/ lpds

eSafety Policy

School Name

Date Created:

Policy Creation and Review

This eSafety Policy has been written as part of a consultation process involving the following people:

.....

It has been approved by Governors and will be monitored and reviewed as listed below:

Policy Created - Date: .....

Intended Policy Review - Date: .....

The implementation of this policy will be monitored by:

.....

This policy will be reviewed as appropriate by:

.....

Approved by ..... (Headteacher)

Date: .....

Approved by ..... (Governor)

Date: .....

Contents

1. Introduction

The Lancashire eSafety Policy Guidance document aims to support you in the creation or update of your school's eSafety Policy. Each school's Policy will be different as it needs to reflect the individual school context and should be updated regularly, at least on an annual basis, or to reflect changing circumstances, purchase of new equipment or incidents within the school.

This document, though not an exhaustive list, will provide prompts / questions for detailed discussion in relation to key eSafety concerns, following which a series of informed Policy decisions can be made. The responses to the questions will form the content of the Policy. Examples of Acceptable Use Policies, forms and letters e.g. for parents, are provided in the appendices. These may not all be relevant to your circumstances and should be amended as necessary to reflect individual school policy decisions.

It is considered good practice to actively involve the whole school community, including children, in the decision making process ensuring that individuals agree with, support and respect decisions rather than feeling restrictions are being imposed unnecessarily.

Your eSafety Policy should be integrated with other relevant school policies, initiatives and documents, for example EYFS framework, behaviour, safeguarding and anti- bullying policies and should form part of your general plans for School Improvement or performance management targets.

In a recent Ofsted document (February 2013 - Information Communication Technology (ICT) survey visits), one of the criteria listed for ICT to be regarded as good/outstanding, is that eSafety is a priority across all areas of the school.

eSafety will naturally tend to focus on reducing the potential risks; however it should equally promote the benefits to be gained from the opportunities afforded through use of technology.

.

Don't forget to promote the positives - Make eSafety a talking point in your school.

Acknowledgements: Lancashire Safeguarding Children Board eSafety Group, SWGfL, Kent NGfL, Plymouth early years team.

2. Your school's vision for eSafety

Your vision statement should summarise your approach to eSafety and outline how this will encourage safer use of technology. It may expand on the school's general mission statement and should be of relevance to the whole school community. In compiling your vision, you should consider:

- Does your school provide a diverse, balanced and relevant approach to the use of technology?
- Are the children encouraged to maximise the benefits and opportunities that technology has to offer?
- Does your school ensure that children learn in an environment where security measures are balanced appropriately with the need to learn effectively?
- Are children equipped with the skills and knowledge to use technology appropriately and responsibly?
- Does your school teach how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment?
- Do all users in your school community understand why there is a need for an eSafety Policy?

3. The school's eSafety Champion

It is recommended that schools appoint an eSafety Champion to be the main point of contact for eSafety related issues and incidents. The choice of eSafety Champion should reflect the school's organisation and preferably be a member of the Senior Leadership Team. However, certain responsibilities may need to be delegated to other staff e.g. Designated Senior Person/Child Protection Officer as necessary.

The role of the eSafety Champion should include:

- Having operational responsibility for ensuring the development, maintenance and review of the school's eSafety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an eSafety incident occur.
- Ensuring an eSafety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with eSafety issues and guidance through liaison with the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging eSafety advice/training for staff, parents/carers and governors.
- Ensuring the Headteacher, SLT, staff, children and governors are updated as necessary.
- Liaising closely with the school's Designated Senior Person / Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

Your eSafety Policy should refer to this nominated person so that all users are aware of the main contact in event of queries or incidents.

4. Security and data management

ICT security is a complex subject that involves all technology users in the school, dealing with issues regarding the collection and storage of data through to the physical security of equipment. The *Lancashire ICT Security Framework* (published 2005) should be consulted to ensure that procedures are in place to ensure data, in its many forms, is kept secure within the school.

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.

All data in your school must be kept secure and staff informed of what they can or can't do with data through the eSafety Policy and statements in the Acceptable Use Policy (AUP).

You should consider these questions:

- Does your school map key information that is held?
- Is there a named person with responsibility for managing information?
- Do relevant staff know the location of data?
- Do all staff with access to personal data understand their legal responsibilities?
- How will your school ensure that data is appropriately managed both within and outside the school environment?
- Are staff aware that they should only use approved means to access, store and dispose of confidential data?
- If staff have remote access to school data, how do you ensure the data remains secure, e.g. are staff aware of the dangers of unsecured wireless access at home?
- Do you allow the use of 'cloud' storage facilities e.g. Dropbox / SkyDrive or external storage related to software used for creation of children's profiles (especially in Early Years)? How do you ensure that data is securely stored and satisfies the requirements of the Data Protection Act?
- What is your school's policy on using mobile devices and removable media? Is this allowed and if so:
    - Is data on these devices password protected and encrypted?
    - Are the devices themselves password protected and encrypted?
    - Are devices containing data allowed to be removed from the school premises?
- How does your school ensure personal devices are not used to access data on school systems e.g. downloading e-mail or files to a Smartphone?
- How does your school ensure the risk of data loss is addressed and managed?
- What is your school's procedure for backing up data?

5. Use of mobile devices

School use of mobile devices, including laptops, tablets, mobile phones, cameras and games consoles is becoming more commonplace. Whilst these can provide a flexible solution and offer a range of exciting opportunities to extend children's learning, their use poses challenges in terms of eSafety. Many of these devices integrate functionality to take images, access the Internet and engage users in various methods of external communication.

Some schools provide devices e.g. iPads for use in class whilst others allow staff (and children) to bring personal devices into school to use as resources for teaching and learning,
The EYFS framework: Section 3.4 (2012) states that
"*….Safeguarding policy and procedures must include an explanation of the action to be taken in the event of an allegation being made against a member of staff,* ***and cover the use of mobile phones and cameras in the setting."***

Each school must consider what is acceptable with regard to the use of mobile phones and cameras. This should be documented in eSafety or Safeguarding Policies and should be cross referenced. In response to the requirements of the EYFS framework, and to avoid confusion or misinterpretation, many schools implement procedures with respect to mobile devices across the whole school. The following sections contain key areas for discussion.

Mobile phones

Mobile phones can present a variety of challenges if not used appropriately and each school must define and document clear boundaries for their use. They are valuable items that can be lost, stolen or damaged in the school environment and could also be considered as distracting or intrusive in a teaching or learning situation. However, staff and parents may equally have valid reasons why mobile phones should be readily available. Rules for the acceptable use of mobile phones should be discussed widely, be communicated to and respected by all users including staff, visitors and parents.

Areas for discussion:

- Do you allow use of personal mobile phones by adults or children in school?
- Do you have designated 'mobile phone free' area(s) where the use of phones is not allowed e.g. toilets or changing areas?
- Do you have designated times when use of personal mobile phones is allowed e.g. lunch or break times?
- Do you require mobile phones to be switched off or 'on silent' during the school day?
- Is there a safe and secure area where personal mobile phones can be stored when not in use e.g. lockers for adults or a requirement for children to take mobile phones to the office for safe storage?
- Are personal mobile phones expected to be security marked, password protected and insured?
- How can children, staff or visitors be contacted in the event of an emergency?
- Do you have very clear statements to say that images, video or audio must not be recorded on a personal mobile phone without specific authorisation from the headteacher?

- Do you allow users to access the Internet via personal mobile phones using the school's wi fi connection (if available)?
- Do you have a 'work' device for staff to use, for example, whilst outside the main buildings or on trips?
- Are users aware of the acceptable, authorised use of a 'works' mobile? How is this use monitored and recorded?
- How do you ensure that the device is always ready for use e.g. fully charged and 'in credit'?
- How are visitors, including parents made aware of your rules for acceptable use of a mobile phone?
- Are staff aware of the potential for mobile phones to be used for cyberbullying? How is cyberbullying approached in your school?
- Are staff aware that they may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy? Do you have clear guidance regarding confiscating and searching the contents of a device or handing over evidence to police if you believe an illegal act has occurred?
- Are staff vigilant in monitoring visitors for any covert use of mobile phones / cameras?
- Do you have a procedure in place for reporting any suspicious use of mobile phones and / or cameras? Are staff familiar with this?
- Are users aware of any 'sanctions' for misuse of mobile phones?

Other mobile devices

The content of this section will reflect the range of mobile devices being used in your school. As new technologies are introduced, their use should be risk assessed and balanced against their potential benefits for learning. If needed, amendments should be made to the eSafety Policy.

General areas for discussion:

- Do you allow use of personal mobile devices in school by adults or children?
- Do you require these devices to have security settings enabled e.g. access passwords?
- Are the device owners aware of their responsibility to ensure all content on these devices is legal and appropriate for a school setting?
- Are device owners aware that the school cannot be held liable e.g. for any damage or theft of personal devices?
- Do you allow personal devices to be connected to the Internet via the school's connection? Is any record maintained of these connections?
- Are devices 'virus checked' (if applicable) before use on school systems?
- How do you ensure physical security of school based devices?

If using tablet devices:

- Have you considered how content will be purchased to comply with copyright legislation?
- How will content be transferred between devices? How will you ensure the safety and security of e.g. email accounts, Bluetooth or 'Cloud storage'?
- Are users aware of any 'sanctions' for misuse of mobile devices?

6. Use of digital media (cameras and recording devices)

The use of cameras and sound recording devices offer substantial benefits to education but equally present schools with challenges particularly regarding publishing or sharing media on the Internet, e.g. on Social Network sites.

Photographs and videos of children and adults may be considered as personal data in terms of The Data Protection Act (1998). To ensure all users are informed about the risks surrounding taking, using, sharing, publishing and distributing digital media, your school should consider the following points for discussion and inclusion in your eSafety Policy.

Consent and Purpose

- Do you have ***written*** consent from parents for photographs of their children to be taken or used? Verbal consent is not considered acceptable.
- Do you have ***written*** consent from adults employed in the setting for their photographs to be taken or used?
- Is it made very clear, when gaining consent, how photographs can / cannot be used (including the use of external photographers or involvement of 3rd parties)?
- Does consent include permission to store / use images once a child has left the school e.g. for brochures, displays etc? Parents should be informed of the timescale for which images will be retained.
- How often is this permission obtained? What procedures are in place for changes in circumstances that may necessitate removal of permission?
- Are parents informed of the purposes for which images may be taken and used e.g. displays, website, brochures, learning journeys and portfolios, press / other external media?
    - Are images displayed in public areas e.g. the entrance hall? What is the 'purpose' of these displays and how are images selected for such a display?
    - Do you need specific parental permission for their child's images to be included in portfolios maintained by trainees / students not directly employed by the setting?
    - Do you need permission to use group images in individual children's profiles e.g. can an image of a group activity in EYFS be included in several children's profiles?
    - How do you ensure that only current images are used, i.e. not children / adults who have left the setting?
- The press have special permissions in terms of Data Protection and may wish to name individual children to accompany a photograph. Do you have written permission from parents for this? At times, the media may publish an image in their online publication which may offer facilities for the 'public' to add comments in relation to a story or image. These can potentially invite negative as well as positive comments. Do you have parental permission for images to be used in a way that supports this?
- How are all adults working in the setting kept informed of any children / other adults whose photographs must not be taken?

Taking Photographs / Video

- Which adults are authorised to take images? This may differ according to their status in the school and be designated by the headteacher.
- Are photographs/videos only taken using school owned equipment? The use of personal equipment to store images should be avoided.
- When taking photographs/ video:
  - Are the rights of an individual to refuse to be photographed respected?
  - Do you ensure that the photograph doesn't show children who are distressed, injured or in context that could be embarrassing or misinterpreted?
  - Do you ensure that certain children are not continually favoured when taking images?
    - Do you ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted? This would include for example, considering the angle of shots for children engaged in PE activities.
    - Are certain areas of the setting 'off limits' for taking photographs, e.g. toilets, cubicles etc.
  - Close up shots should be avoided as these may be considered intrusive. Shots should preferably include a background context and show children in group situations.

Parents Taking Photographs / Videos

- Under the Data Protection Act (1998), parents are entitled to take photographs of ***their own*** children on the provision that the images are for ***their own*** use, e.g. at a school production. Including other children or other purpose could constitute a potential breach of Data Protection legislation.
- Are parents informed that they should only take photographs of their own children and that they need permission to include any other children / adults?
- Are parents reminded, preferably in writing, that publishing images which include children other than their own or other adults on Social Network sites is not acceptable, unless specific permission has been obtained from the subjects?
- Do you have / need a request form that 'allows' parents to use cameras at a specified time / in a designated area for a particular purpose?
- Are parents encouraged to be considerate when taking photographs, e.g. not obscuring the view of others or being intrusive?

Storage of Photographs / Video

- How do you ensure that photographs are securely stored and not removed from the school environment? This could include storage of images on portable devices e.g. laptops or tablets.
- Do you allow images to be stored on USB memory sticks? Are such mobile devices encrypted or password protected?
- Do you 'store' images on tablets, 'apps' or use 'Cloud' storage? Are you confident that your images are being stored securely if hosted outside the setting?
- Are parents / carers informed if images are to be stored outside the school setting?
- Do you allow staff to store images on personal equipment e.g. tablets, laptops or USB storage devices?
- Do you allow staff to store personal images on school equipment?
- Who has access to photographs / videos stored on your equipment?
- Who is responsible for deleting photographs / video or disposing of printed copies (e.g. by shredding) once the purpose for the image has lapsed?
- How do you ensure images are disposed of should a parent withdraw permission?

- If you 'send' photographs electronically e.g. via email, how do you ensure that the email is secure?

Publication of Photographs / Videos

- Consent is needed from parents for publication of children's images, e.g. on a website.
- Photographs should only be published online to secure sites.
- When publishing photographs, care should be taken over the choice of images to ensure that individual children / adults cannot be identified or their image made available for downloading or misuse, e.g. through the use of low definition images that will not magnify effectively.
- Full names and / or other personal information should not accompany published images.

When publishing images,

- How do you ensure that children's images are not displayed on insecure sites e.g. personal Social Networking Sites?
- Are staff and children aware that full names and personal details will not be used on any digital media, particularly in association with photographs?
- Do all staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites? Staff should ensure that personal profiles are secured and do not display content that is detrimental to their own professional status or could bring the school into disrepute.

The Media, 3rd Parties and Copyright

Are 3rd Parties supervised at all times whilst in the school and able to comply with the Data Protection requirements in terms of taking, storage and transfer of images?

- Who owns the copyright for images taken by a 3rd party?
- If uploading images to a 3rd party website, e.g. for printing or creating calendars, cards etc, have you read the terms and conditions of the web site. You could unknowingly be granting the site's host licence to modify copy or redistribute your images without further consent. The site may also be advertised for 'personal use' only – therefore using for business purposes would be a breach of the terms and conditions.

CCTV, Video Conferencing, VOIP and Webcams

- Parents should be informed if CCTV, video conferencing or webcams are being used in use in the school.
- Have parents given permission for their child/children to participate in activities that include taking of video and photographs? Although children may not be appearing 'live' on the Internet through a video conferencing link, it is still important to remember that the images which are broadcast from school could be captured as a snapshot or video clip from a system receiving the broadcast.
- Are video conferencing (or similar) sessions logged including the date, time and the name of the external organisation/ person(s) taking part?
- Are notifications in place to inform setting users that CCTV is being used?
- Is the purpose for using CCTV /video conferencing or webcams made clear to those liable to be included in footage taken by these resources?
- Where are the cameras located? Do they overlook sensitive areas, e.g. changing rooms or toilets?
- Who has access to recordings? How are these stored and erased?

- How will you ensure that copyright, privacy and Intellectual Property Rights (IPR) legislation are respected?
- How will you ensure that recordings are not repurposed in any other form or media other than the purpose originally agreed?

Examples of Image Consent forms can be found in the Appendices. These should be adapted to reflect your school's context and policy.

7. Communication technologies

Schools use a variety of communication technologies and need to be aware of the benefits and associated risks. New technologies should be risk assessed against the potential benefits to learning and teaching before being employed throughout the school. Ideally this should be done before multiple devices are purchased. As new technologies are introduced, the eSafety Policy should be updated and all users made aware of the changes.

The following are examples of commonly used technologies which you may want to include in your policy.

Email

The following statements / questions reflect safe practice in the use of email. You may want to adopt/adapt some of these for inclusion in your school policy.

- It is recommended that all users have access to the Lancashire Grid for learning service as the preferred school email system.
- What is your policy on staff use of personal email accounts during school hours, on school equipment or for professional purposes?
- Do you have email accounts for children? How are these organised e.g. class, group or project accounts?
- Can children potentially be identified through their email address e.g. **john.smith@class6.myschool.co.uk** ?
- Only official email addresses should be used to contact staff or children.
- The Lancashire Grid for Learning filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to 'One Connect'.
- Are all users aware of the risks of accessing content including SPAM, phishing, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school?
- Are all users 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?
- Are all users aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy?
- How will the content of children's email communications be monitored?
- How should users report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature?
- Are users aware that they should not open attachments that they suspect may contain illegal content as they could inadvertently be committing a criminal act?

- Your school may elect to include a standard disclaimer at the bottom of all outgoing email communications (see example below).

Example school e-mail disclaimer:

This e-mail and any files transmitted within it may be confidential and are intended solely for the individual to whom it is addressed. Any views or opinions presented are those of the author and do not necessarily represent xxxxxxxxxx School. If you are not the intended recipient, you must not use, disseminate, forward, print or copy this e-mail or its contents. If you have received this e-mail in error, please contact the sender. Please note that e-mail may be monitored in accordance with both school policy and the Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000.

Social Networks

Social Network sites allow users to be part of a virtual community. Current popular examples of these sites are Facebook, Twitter, Club Penguin and Moshi Monsters (for children). These sites provide users with simple tools to create a profile or page including basic information about themselves, photographs, and possibly a blog or comments. As a user on a Social Network site, you may have access to view other users' content, send messages and leave unmediated comments. Many Social Network sites are blocked by default through filtering systems used in schools, but these settings can be changed at the discretion of the headteacher (See **http://www.lancsngfl.ac.uk/lgfladvice/index.php** for more details).

Although use of Social Networks tends towards a personal basis outside of the school environment, their use as a tool for communicating with parents is becoming more commonplace in primary schools. It is recommended that guidance for personal use of social networking, and personal publishing sites is included as part of staff induction, discussed regularly and outlined in the staff Acceptable Use Policy – along with sanctions for inappropriate use.

If a school Social Network page is to be created, you must consider the purpose and audience and also ensure that the privacy settings and interaction are appropriate.

Remember; whatever methods of communication are used, individuals should always conduct themselves in a professional manner. If content is made available on the web it is available for everyone to see and potentially remains there forever.

All staff need to be made aware of the following points:

- The content on Social Network sites may be unmediated and inappropriate for certain audiences.
- If a Social Network site is used personally, details must not be shared with children and privacy settings be reviewed regularly to ensure information is not shared automatically with a wider audience than intended.
- They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- The content posted online should not :
    - bring the school into disrepute
    - lead to valid parental complaints
    - be deemed as derogatory towards the school and/or its employees

    - be deemed as derogatory towards pupils and/or parents and carers
    - bring into question their appropriateness to work with children and young people.
- Adults must not communicate with children using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted. Online Communications with parents, past pupils or siblings of pupils, especially if under the age of 18 should be discouraged.
- Children must not be added as 'friends' on any Social Network site.

The school should also consider the advice they provide for parents in terms of their use of Social Networking Sites and how the school will respond to identified issues. Common concerns that may need consideration include:

- Posting inappropriate comments about staff or children that could be construed as instances of cyberbullying.
- Posting images of children or adults on profiles without permission of the individuals involved, especially if the photographs contain children other than their own.

Instant Messaging or VOIP

Instant Messaging systems, e.g. Text messaging, Skype, Facetime, are popular communication tools with both adults and children. They can provide an opportunity to communicate in 'real time' using text, sound and video. The Lancashire Grid for Learning filtering service 'blocks' some of these sites by default, but access permissions can be changed at the request of the headteacher (See **http://www.lancsngfl.ac.uk/lgfladvice/index.php** for more details).

Your school should consider:

- Are staff and children aware of the risks involved using this technology e.g. viewing inappropriate images or making unsuitable contacts?
- Do you allow staff to use school equipment to communicate with personal contacts e.g. through 'Facetime' on an iPad?
- Do you make use of more secure messaging, forum or chat systems within their VLE (e.g. Moodle)?
- If the school uses text messaging to contact parents, how is the security of messages and data e.g. contact lists ensured?

Virtual Learning Environment (VLE) / Learning Platform

Various systems, e.g. Moodle are being used regularly in schools as communication tools.

Your school should consider:

- How you manage the use of communication tools within the VLE.
- Who is given access and at what level?
- How passwords are issued and their security maintained.
- Which tools children are allowed to access.
- How children are taught to use these communication tools in a responsible way in conjunction with the eSafety curriculum.
- Whether teachers know how to monitor the use of these tools.

- If accounts are deleted when staff and children leave the school. Is this monitored and by whom?

Websites and other online publications

This may include for example, school websites, Social Network profiles, podcasts, videos, wikis and blogs.

Information posted online is readily available for anyone to see and thus form an opinion about the school. From September 2012, the School Information (England) (Amendment) Regulations 2012 specified that certain up to date information must be made available on a school's website. More details regarding these requirements can be found on the DfE website or at **http://www.legislation.gov.uk/uksi/2012/1124/made**

Your school should consider:

- Is your school website or online publication effective in communicating eSafety messages to parents/carers?
- Is everybody in the school made aware of the guidance for the use of digital media on the website / online publication?
- Is everybody in the school aware of the guidance regarding the inclusion of personal information on the website/ online publication?
- Who has access to edit online publications and ensure that the content is relevant and current?
- Who has overall responsibility for what appears on the website?
- Is any content subject to copyright/personal intellectual property restrictions?
- Does any of the content need to be hidden behind a password protected area?
- Are downloadable materials in a read-only format (e.g. PDF) where necessary, to prevent content being manipulated and potentially re distributed without the school's consent?

8. Infrastructure and technology

Your school must ensure that the infrastructure/network is as safe and secure as possible. For schools subscribing to the Lancashire Grid for Learning/CLEO Broadband Service, internet content filtering is provided by default. It is important to note that the filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service. Sophos Anti-Virus software is included in the school's subscription, but this needs to be installed on computers in school and then configured to receive regular updates. Further information can be found at **www.lancsngfl.ac.uk/esafety** .

Your school needs to consider what guidance is offered regarding the following security issues:

Children's access

- How are children supervised when accessing school equipment and online materials (e.g. working with a trusted adult)?
- What access do children have to the school systems e.g. individual or class logins?
- Is children's access restricted to certain areas of the network?

Adult access

- Is access to school systems available for all staff or restricted according to their areas of responsibility?

Passwords

- Are all staff aware of the guidelines in the Lancashire ICT Security Framework for Schools? This is available at **www.lancsngfl.ac.uk/esafety** website.
- Do all users of the school network have a secure username and password?
- Is the administrator password for the school network available to the headteacher or other nominated senior leader and kept in a secure place e.g. school safe?
- Are staff and children reminded of the importance of keeping passwords secure?
- How often will passwords be changed?
- Is there an agreed format for creating passwords e.g. mixture of letters, numbers and symbols?

Software/hardware

- Do you have legal ownership of all software (including apps on tablet devices)?
- Do you have an up to date record of appropriate licenses for all software and who is responsible for maintaining this?
- Do you regularly audit equipment and software?
- Who controls what software is installed on school systems?

Managing the network and technical support

- Are servers, wireless systems and cabling securely located and physical access restricted?
- Have all wireless devices had security enabled?
- Are wireless devices accessible only through a secure password?
- Have relevant access settings been restricted on tablet devices e.g. downloading of apps or 'in-app' purchases?
- Who is responsible for managing the security of your school network?
- How often do you review the safety and security of your school network?
- How are school systems kept up to date in terms of security e.g. are computers regularly updated with critical software updates/patches?
- Do users (staff, children, guests) have clearly defined access rights to your school network e.g. do they have a username and password and how are permissions assigned?
- Are staff and children required/reminded to lock or log out of a school system when a computer/digital device is left unattended?
- Are any users allowed to download executable files or install software? If not, who is responsible for assessing and installing new software?
- How do users report any suspicion or evidence of a breach of security? Is there a named person with overall responsibility?

- What is your school's guidance on using removable storage devices on school e.g. encrypted pen drives?
- What is your school's guidance on using school equipment e.g. teachers laptop for personal/family use?
- If network monitoring takes place, is it in accordance with the Data Protection Act (1998)?
- Are staff made aware of all network monitoring and/or remote access that takes place and by whom?
- Are all internal/external technical support providers aware of your schools requirements / standards regarding eSafety?
- Who is responsible for liaising with/managing the technical support staff?

Filtering and virus protection

- Has the school requested devolved control over the LGfL filtering service? (See **http://www.lancsngfl.ac.uk/lgfladvice/index.php** for more details.)
- How is the filtering managed and by whom?
- Where is information regarding devolved filtering stored in school? This needs to be available for any new member of the SLT.
- How is devolved filtering communicated to members of staff?
- Are staff aware of the procedures for blocking and unblocking specific websites?
- What procedures are there in place to ensure that ALL equipment including school laptops used at home are regularly updated with the most recent version of virus protection software used in school?
- Are staff aware of the procedures for reporting suspected or actual computer virus infection?

9. Dealing with incidents

Your school needs to consider the types of incident that may occur and how these will be dealt with. An incident log (see Appendix 11) should be completed to record and monitor offences. This must be audited on a regular basis by the eSafety Champion or other designated member of the Senior Leadership Team.

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the headteacher 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 12). 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

It is more likely that your school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions are proportionate to the offence. Your school must decide what constitutes inappropriate use and the sanctions to be applied. Some examples of inappropriate incidents are listed below with suggested sanctions.

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.	

Your school should consider:

- Who is responsible for dealing with eSafety incidents? This may involve more than one person for example, eSafety Champion, ICT coordinator, Child Protection Officer, PSHE coordinator.
- Are **all** staff aware of the different types of eSafety incident and how to respond appropriately e.g. illegal or inappropriate.
- What procedures are in place to deal with eSafety incidents and are all staff aware of these?
- How are children informed of the procedures?
- Where these incidents are logged. (See Appendix 11)
- How incidents are monitored, by whom and how frequently.
- What measures are in place to respond to and prevent recurrence of an incident.
- At what point parents or external agencies are involved.
- The procedures that are in place to protect staff and escalate a suspected incident/allegation involving a staff member.

You may want to use the 'eSafety Incident/ Escalation Procedures' document (See Appendix 12) as a framework for responding to incidents.

The school's Behaviour Policy should outline policy and procedures relating to the powers of 'search' referred to in the Education Act (2011). Items 'banned' in school may include for example, electronic devices such as mobile phones. Schools may want to cross reference these procedures in their eSafety Policy.

10. Acceptable Use Policy (AUP)

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

AUPs are recommended for Staff, Children and Visitors/Guests and must be signed and adhered to by users before access to technology is allowed. You may wish to consider this agreement as a partnership between parents/carers, children 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.

A set of exemplar AUPs are provided in the appendices and you may find it helpful to refer to these and the additional points below when writing your school's AUP.
Your school AUPS must:

- Reflect the content of the school's wider eSafety Policy.
- Be regularly reviewed and updated
- Be regularly communicated to all users, particularly when changes are made to the eSafety Policy/AUP.
- Be understood by each individual user and relevant to their setting and role/ responsibilities.
- Outline/summarise acceptable and unacceptable behaviour when using technologies as defined in the wider eSafety Policy.
- Outline the ways in which users are protected when using technologies e.g. passwords, virus protection and filtering.
- Provide advice for users on how to report any failings in technical safeguards.
- Clearly define how monitoring of network activity and online communications will take place and how this will be enforced.
- Outline sanctions for unacceptable use and make all users aware of the sanctions (this may be linked to your Behaviour Policy).
- Stress the importance of eSafety education and its practical implementation.
- Highlight the importance of parents/carers reading and discussing the content of the AUP with their child.

11. Education and training

In 21st Century society, both adults and children need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that children are taught to use technology responsibly, securely and safely, being able to recognise potential risks and knowing

how to respond. They should, for example, be able to communicate safely and respectfully online, be aware of the necessity to keep personal information private, be taught how to search effectively and be discerning in their evaluation of digital content and be aware of the need to respect copyright and Intellectual Property rights.

The three main areas of eSafety risk (as mentioned by OFSTED, 2013) that your school needs to be aware of and consider are:

Area of Risk	Example of Risk
Content: Children need to be taught that not all content is appropriate or from a reliable source.	• Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse. • Lifestyle websites, for example pro-anorexia/self-harm/suicide sites. • Hate sites. • Content validation: how to check authenticity and accuracy of online content.
Contact: Children need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	• Grooming • Cyberbullying in all forms • Identity theft (including 'frape' - hacking Facebook profiles) and sharing passwords.
Conduct: Children need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others.	• Privacy issues, including disclosure of personal information, digital footprint and online reputation • Health and well-being - amount of time spent online (internet or gaming). • Sexting (sending and receiving of personally intimate images). • Copyright (little care or consideration for intellectual property and ownership – such as music and film).

(Ofsted, 2013, Inspecting eSafety – guidance document)

eSafety - Across the curriculum

It is vital that children are taught how to stay safe, protect themselves from harm and take a responsible approach to their own and others' eSafety.

Your school needs to provide relevant, flexible and engaging eSafety education to all children as part of their curriculum entitlement and consider the following points:

- Do you provide regular, planned eSafety teaching within a range of curriculum areas (using the Lancashire ICT Progression document)?
- How do you ensure eSafety education is progressive throughout the school?
- How will eSafety education be differentiated for children with special educational needs?
- Do you have an additional focus on eSafety during the National eSafety Awareness Week?
- How do you ensure children are made aware of the relevant legislation when using the Internet e.g. Data Protection Act (1998) and copyright implications?
- Are children made aware of the impact of cyberbullying and how to seek help if they are affected by these issues, e.g. using peer mentoring or worry boxes?
- Are children taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions?
- Do you ensure that children develop an understanding of the importance of the Acceptable Use Policy and are encouraged to adopt safe and responsible use of ICT both within and outside school?
- How are children reminded of safe Internet use e.g. classroom displays, eSafety rules (See Appendices), acceptance of site policies when logging onto the school network /Virtual Learning Environment?

eSafety – Raising staff awareness

Your school needs to consider:

- If a staff training needs audit has been carried out to ascertain the level of knowledge and expertise in the use of new technologies and their potential benefits and risks.
- If there is a planned programme of formal eSafety training for all teaching and non-teaching staff to ensure they are regularly updated on their responsibilities as outlined in your school policy?
- Who will provide advice/guidance or training to individuals as and when required e.g. eSafety Champion or other nominated person.
- If members of staff delivering eSafety training received external eSafety training/updates from external or accredited providers?
- Do any of your staff have accredited eSafety qualifications e.g. EPICT or CEOP Ambassador?
- Does eSafety training ensure staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites?
- That all staff are expected to promote and model responsible use of ICT and digital resources.
- Is eSafety training provided within an induction programme for all new staff to ensure that they fully understand both the school's eSafety Policy and Acceptable Use Policy?
- If regular updates on eSafety Policy, Acceptable Use Policy, curriculum resources and general eSafety issues are discussed in staff/team meetings.
- How is the impact of training monitored?

eSafety – 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).

Does your school offer regular opportunities for parents/carers and the wider community to be informed about eSafety, including the benefits and risks of using various technologies both at home and at school? Your school needs to consider how this will be done, for example through:

- School newsletters, homework diaries, Website, VLE/Moodle and other publications.
- Bespoke Parents eSafety Awareness sessions or workshops (held regularly on various days and times, cluster sessions).
- Promotion of external eSafety resources/online materials.

eSafety – Raising Governors' awareness

Your school needs to consider how Governors, particularly those with specific responsibilities for eSafety, ICT or child protection, are kept up to date. This may be through discussion at Governor meetings, attendance at Local Authority Training, CEOP or internal staff/parent meetings.

NB: The eSafety Policy should be regularly reviewed and approved by the governing body.

12. Evaluating the impact of the eSafety Policy

It is important that schools monitor and evaluate the impact of safeguarding procedures throughout schools.
Your school should consider:

- How will you know if your eSafety Policy is having the desired effect?
- How are eSafety incidents monitored, recorded and reviewed?
- Who is responsible for monitoring, recording and reviewing incidents?
- Is the introduction of new technologies risk assessed?
- Are these assessments included in the eSafety Policy?
- Are incidents analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children?
- How can these patterns be addressed most effectively e.g. working with a specific group, class assemblies, reminders for parents?
- How does the monitoring and reporting of eSafety incidents contribute to changes in policy and practice?
- How are staff, parents/carers, children and governors informed of changes to policy and practice?
- How often are the AUPs reviewed and do they include reference to current trends and new technologies?

Appendices

APPENDIX 1
Example of Image Consent Letter to Parents

<Insert School's Letterhead>

Dear Parent / Carer

We regularly take photographs/videos of children at our school and believe that these can provide a valuable record of children's learning. These may be used in children's learning journeys and profiles, our school prospectus, in other printed publications, on our school website/VLE, or in school displays, including digital photo frames. (*List any other specific uses here).*

We also actively encourage children to use school cameras to take photographs / videos as part of their learning activity.

Occasionally, our school may be visited by the media or third party who will take photographs/videos of an event or to celebrate a particular achievement. These may then appear in local or national newspapers, websites or on televised news programmes.

We recognise that increased use of technology and opportunities for online publishing mean that there is greater potential for accidental or deliberate misuse. We endeavour to minimise risks by putting safeguards in place that will protect your child's interests, and enable us to comply with the Data Protection Act (1998).

Please read and complete the attached consent form (for each child) and return to school as soon as possible. We appreciate that some families may have additional concerns and anxieties regarding protection of a child's identity and therefore request that you inform us, in writing, of any special circumstances either now or at any time in the future that may affect your position regarding consent.

Yours sincerely,

Headteacher

APPENDIX 2
Image Consent Form

Name of the child's parent/carer:.....

Name of child:.....

Year group:.....

Please read the Conditions of Use on the back of this form then answer questions 1-4 below. The completed form (one for each child) should be returned to school as soon as possible. (Please Circle your response)

1. Do you agree to photographs / videos of your child being taken by authorised staff within the school? Yes / No

2. Do you agree to photographs / videos of your child being taken in group situations by 3rd parties at special events e.g. School productions or extra curricular events? Yes / No

3. May we use your child's image in printed school publications and for digital display purposes within school? Yes / No

4. May we use your child's image on our school's online publications e.g. website / blog / VLE? Yes / No

5. May we record your child on video? Yes / No

6. May we allow your child to appear in the media as part of school's involvement in an event? Yes / No

I have read and understand the conditions of use attached to this form

Parent/Carer's signature: .....

Name (PRINT): .....

Date: .....

Conditions of Use

1. This form is valid for this academic year <*insert dates*>.
2. The school will not re-use any photographs or videos after your child leaves this school without further consent being sought.
3. The school will not use the personal contact details or full names (which means first name **and** surname) of any pupil or adult in a photographic image, or video, on our website/VLE or in any of our printed publications.
4. If we use photographs of individual children, we will not use the full name of that pupil in any accompanying text or caption.
5. If we use the full name of a pupil in the text, we will not use a photograph of that pupil to accompany the article.
6. We will only use images of children who are suitably dressed and in a context that is not open to misinterpretation.
7. 3rd Parties may include other children's parents or relatives e.g. attending a school production.
8. Images / videos will be stored according to Data Protection legislation and only used by authorised personnel.
9. Parents should note that websites can be viewed throughout the world and not just in the United Kingdom, where UK law applies.

Notes on Use of Images by the Media

If you give permission for your child's image to be used by the media then you should be aware that:

1. The media will want to use any images/video that they take alongside the relevant story.
2. It is likely that they will wish to publish the child's full name, age and the school's name in the caption for the picture (possible exceptions to this are large group or team photographs).
3. It is possible that the newspaper will re-publish the story on their website or distribute it more widely to other newspapers or media organisations.

APPENDIX 3
Example Consent Form for Images to be Taken e.g. at a School Production or Special Event

Dear Parent/ Carer,

Your child will be appearing in our school production / event name on <*insert date/s*>. We are aware that these events are special for children and their relatives / friends and form treasured memories of their time at school.

We have a rigorous policy in place with regard to taking, using and publishing images of children and you have already signed a consent form stating whether you agree to your child's images / video being used in general circumstances.

Many parents / carers like to take photographs / videos of their children appearing in school productions, but there is a strong possibility that other children may be included in the pictures. In these circumstances, we request specific consent for images / videos to be taken by a third party (i.e. other parents). We need to have permission from all parents / carers of children involved in the production to ensure that they are happy for group images / videos to be taken and I would be grateful if you could complete the slip at the bottom of this letter and return to school as soon as possible.

We would also request that images / videos including other children or adults are not posted online, especially on Social Media sites e.g. Facebook without the specific permission of the individuals included in the footage.

Should any parents / carers not consent, we will consider other options, e.g. arranging specific photo opportunities after the production.

These decisions are not taken lightly, but we have to consider the safeguarding of all our children and respect parents' rights to privacy.

Yours sincerely,
Headteacher.

Child's name: _____ Date: _____

I agree / do not agree to photographs / videos being taken by third parties at the <*insert event*> *on* <*Insert date /s*>.

Signed _____ *(Parent / Carer)*

Print name _____

APPENDIX 4
Example of ICT Acceptable Use Policy (AUP) – Staff and Governors

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the headteacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in eSafety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with children and other adults are appropriate.
8. I will not use the school system(s) for personal use during working hours.
9. I will not install any hardware or software without the prior permission of <*insert name*>.
10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
12. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
13. I will report any known misuses of technology, including the unacceptable behaviours of others.
14. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
15. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
16. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

17. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
18. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
19. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's eSafety policy and help children to be safe and responsible in their use of ICT and related technologies.
20. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature .....

Date .....

Full Name .....(PRINT)

Position/Role .....

APPENDIX 5
Example of ICT Acceptable Use Policy (AUP) – Students, Supply Teachers, Visitors, Guests etc.

To be signed by any adult working in the school for a short period of time.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
3. I will not use any external device to access the school's network e.g. pen drive.
4. I will respect copyright and intellectual property rights.
5. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
6. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
7. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
8. I will not install any hardware or software onto any school system.
9. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature
I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature .....

Date .....

Full Name .....(PRINT)

Position/Role .....

Appendix 6
Example of ICT Acceptable Use Policy (AUP) - Children

These rules reflect the content of our school's eSafety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

- ✓ I will only use ICT in school for school purposes.
- ✓ I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher.
- ✓ I will only use the Internet and/or online tools when a trusted adult is present.
- ✓ I will only use my class e-mail address or my own school email address when emailing.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- ✓ I will not deliberately bring in inappropriate electronic materials from home.
- ✓ I will not deliberately look for, or access inappropriate websites.
- ✓ If I accidentally find anything inappropriate I will tell my teacher immediately.
- ✓ I will only communicate online with people a trusted adult has approved.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not give out my own, or others', details such as names, phone numbers or home addresses.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will not arrange to meet anyone that I have met online.
- ✓ I will only open/delete my own files.
- ✓ I will not attempt to download or install anything on to the school network without permission.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.
- ✓ I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy.
- ✓

.....**Parent/ Carer Signature**

We have discussed this Acceptable Use Policy and
..... [Print child's name] agrees to follow the eSafety rules and to support the safe use of ICT at <*insert school name*>l.

Parent /Carer Name (Print) .....

Parent /Carer (Signature) ....

Class ..... Date.....

This AUP must be signed and returned before any access to school systems is allowed.

APPENDIX 7
ICT Acceptable Use Policy (AUP) – Example Parent's Letter

<Insert School's Letterhead>

Dear Parent/Carer,

The use of ICT including the Internet, e-mail, learning platforms and mobile technologies are integral elements of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all children to act safely and responsibly when using technology both within, and outside of, the school environment.

In school, we ensure that all resources used by the children are age appropriate and suggest that parents check the terms and conditions for the use of online resources and games to ensure that resources used at home are also age appropriate. This is particularly relevant when using Social Network Sites that incorporate age-restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of the site's privacy policy and / or terms and conditions and therefore we actively discourage this in our school.

The enclosed ICT Acceptable Use Policy forms part of the wider School eSafety Policy and alongside the school's Behaviour and Safeguarding Policies outlines those principles we expect our children to uphold for the benefit of both themselves and the wider school community.

Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible. Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguard the children in school.

Along with addressing eSafety as part of your child's learning, we will also be holding Parental eSafety Awareness Sessions during the school year and I would take this opportunity to strongly encourage your attendance wherever possible. Further information on these sessions will be communicated as soon as dates are confirmed. In the meantime, if you would like to find out more about eSafety for parents and carers, please visit the Lancsngfl eSafety website http://www.lancsngfl.ac.uk/esafety

If you have any concerns or would like to discuss any aspect of the use of ICT in school, please contact <*insert school contact person*>.
Yours sincerely,

<*The Headteacher*>

APPENDIX 8
Example of Typical Classroom eSafety Rules (EYFS/KS1)

Our Golden Rules for Staying Safe with ICT

We only use the Internet when a trusted adult is with us.

We are always polite and friendly when using online tools.

We always make careful choices when we use the Internet.

We always ask a trusted adult if we need help using the Internet.

We always tell a trusted adult if we find something that upsets us.

APPENDIX 9
Example of Typical Classroom eSafety Rules (KS2)

Our Golden Rules for Staying Safe with ICT

We always ask permission before using the internet.

We only use the Internet when a trusted adult is around.

We immediately close/minimise any page we are uncomfortable with (or if possible switch off the monitor).

We always tell an adult if we see anything we are uncomfortable with.

We only communicate online with people a trusted adult has approved.

All our online communications are polite and friendly.

We never give out our own, or others', personal information or passwords and are very careful with the information that we share online.

We only use programmes and content which have been installed by the school.

APPENDIX 10
Example of Letter to Parents Regarding Parental eSafety Awareness Session

<Insert School's Letterhead>

Dear Parent/Carer,

Having access to online information and the opportunities that the digital world can offer has many benefits and for some it plays an important part of our everyday lives. However, as technology moves on at such a pace, it is sometimes difficult to keep up with new trends and developments, particularly with regard to mobile/games technologies and secure and safe accessibility to online material.

Our school has policies in place to ensure our children are learning in a safe and secure environment which includes being safe online. This session has been organised to help you to contribute to the process of helping your child to be aware of the potential risks associated with using the Internet and modern technologies.

Ofsted increasingly view Parental eSafety Awareness sessions as essential components of effective safeguarding provision and I would therefore appreciate your support in attending this event.

We will be hosting the above session on the Date/Time below and I would strongly encourage your attendance:

Date:.....Time:.....

The session will include reference to the following areas with time for you to ask questions:

- ✓ What are our children doing online and are they safe?
- ✓ Do they know what to do if they come across something suspicious?
- ✓ Are they accessing age-appropriate content?
- ✓ How can I help my child stay safe online?
- ✓

The session will last for approximately 1¼ hrs where a member of the Local Authority Schools' ICT Team will address the issues mentioned above.

Yours sincerely,

<*The Headteacher*>

.....

I / we will be attending the above Parental eSafety Awareness Session

Name(s):.....

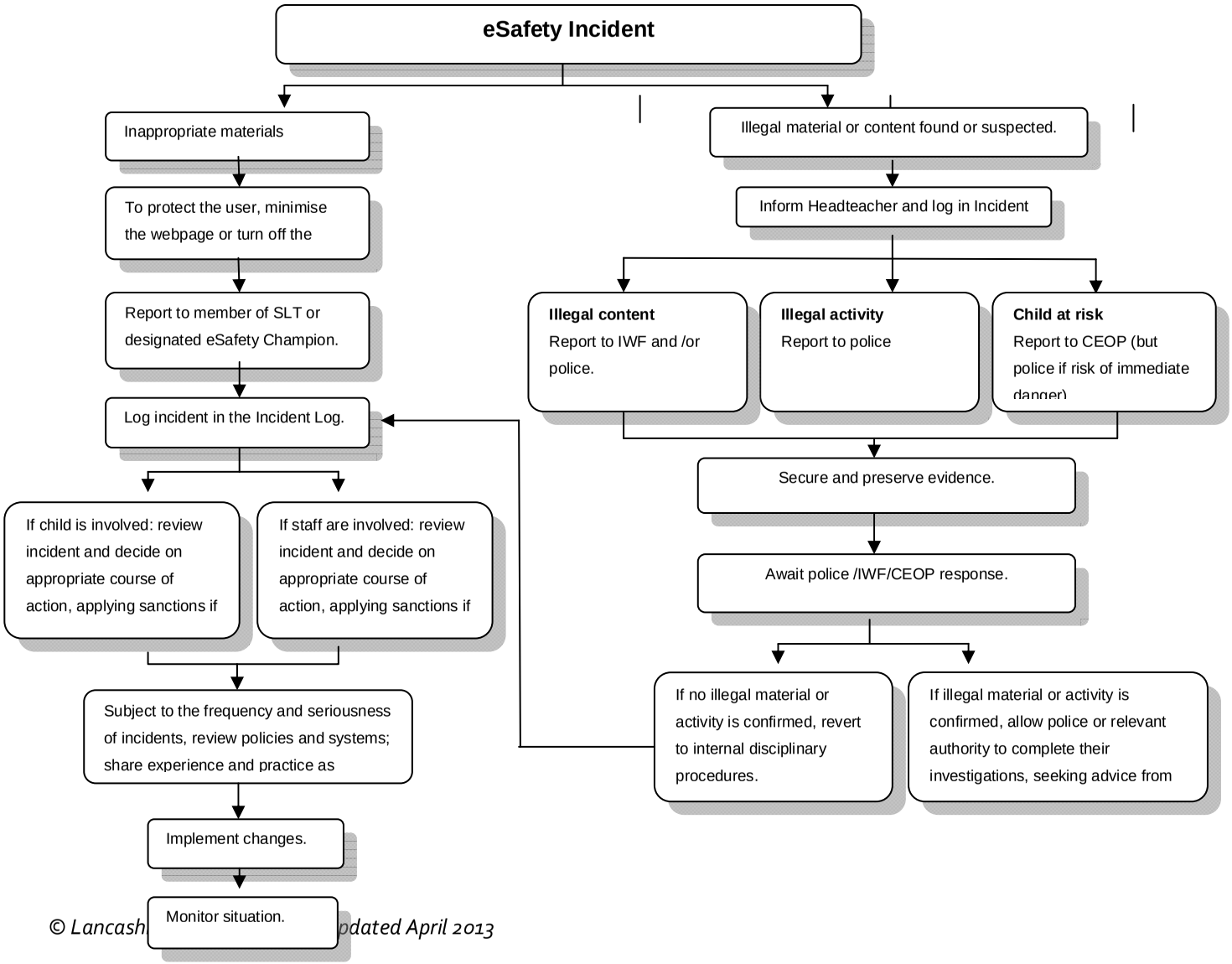
Parent / Carer of:.....*Year Group*.....

APPENDIX 11
Example eSafety Incident Log

All eSafety incidents must be recorded by the School eSafety Champion or designated person. 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.

APPENDIX 12
Responding to eSafety Incident/ Escalation Procedures



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.

 pdated April 2013