Monkhouse Primary School

Primary e-Safety Framework Document

Monkhouse Primary School

Written by L Baggett with support from Neil Brown (LA ICT School Improvement Advisor)
Reviewed by Steven Smith

Reviewed Jan 2017

Developing and Reviewing this Policy

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

The staff and parents of Monkhouse Primary School

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

Policy Reviewed- Date: November 2013

The implementation of this policy will be monitored by ICT co-ordinator & the SMT

This policy will be reviewed as appropriate by ICT coordinator in Nov 2014

Approved by …… (Headteacher) Date ……

Approved by …… (Governor) Date ……

Contents

eSafety Policy 2013 Monkhouse Primary School

1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, 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 eSafety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our eSafety 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. Our school's vision for eSafety

In our school children are safe, happy and ready to take an active role in their learning. We want technology to become integral part in the learning process. Technology will be used to enhance opportunities so teaching and learning is adventurous, ambitious, exciting and set in real life contexts. We aim to focus on developing curiosity, imagination, exploration and investigation, using developing technology, identifying the 'safe way to learn and understand the associated risks. Our teaching will provide children and the school community with the skills and knowledge to use technology appropriately and responsibly both inside and outside school.

3. The role of the school's eSafety Champion

The role of the eSafety Champion in our school includes:

- Ensuring e-safety knowledge and understanding is taught and embedded in teaching and learning at appropriate age levels through all key phases in school.
- 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 the eSafety Incident Log is appropriately maintained and regularly reviewed. (This is kept in the central location of the school office.)

- Keeping personally up-to-date with eSafety issues and guidance through liaison with the Local Authority Schools" ICT Team 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.

Our eSafety Champions are:-

E-Learning lead teacher and Digital Leaders

However, certain responsibilities may need to be delegated to other staff e.g. Designated Senior Person/Child Protection Officer as necessary.

4. Policies and practices

This eSafety policy should be read in conjunction with the following other related policies and documents:

Teaching and Learning Policy

Curriculum policies

CP policy

Safeguarding Policy

4.1 Security and data management

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:

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 key information is recorded and kept in a secure place in the administrative office. The SBM is the named person responsible for managing the information. All staff are clear on their legal responsibilities when they access personal data. No personal data will be permanently stored on individual removable storage devices. All staff are aware that when accessing data at home they use a secure wireless system. All electronic data (assessment information) is accessed by staff using a secure password system. Where possible password or encrypted storage devices will be used to store data.

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:

Any USB device, MP3 players, Mobile Phones, Tablet devices such as iPads.

- Monkhouse Primary School does not prohibit the use of mobile devices on the school network. However, users should note the following items. These examples are for clarification. They are not exclusive.

- Any mobile device must be checked for viruses and spam content before being attached to the school network.

- Mobile devices must not be used to take photographs or sound clips of any person who is unaware of the action and who has not given their permission. Photographs/images of children should not be stored on any of these devices.

- Any use of mobile technology to intimidate, bully, harass or threaten others will be counted as an infringement of network use. This may result in disconnection from the network or legal or civil disciplinary action. Uploading images and sound is only permissible if the subject involved gives permission.

- Any images that involve children must not identify children by name and permission must have been agreed by the relevant parent / carer before posting. A record should be made of who will be taking the photos, why the photos are being taken, when they are being taken and what they are to be used for. This should all be documented in the risk assessment carried out before a school trip or event. The photos should then be stored in a safe area within the school LAN and only used for legitimate educational purposes as directed by the Headteacher.

- Whilst teaching in school all mobile phones must be switched to silent during the hours of 8.45 and 12pm and 1pm – 3.45pm .

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.

Our Using images of children: Photographs, videos, websites, mobile phones and webcams policy clearly sets out the consent from pupils, parents and staff.

- Parent's permission is sought when they enter school. They can agree to aspects of photographs being used in school and beyond. Parents can withdraw their consent at any time.

- Once children have left the establishment any photographs of them are deleted unless they have been used in school documentation where consent has been given.

- A list of consent for photographs is provided to each teacher annually and updated by the office staff where consent changes.

- Parents may take video and photographs of their child engaged in school events for their personal use. Any attempt to publish them on any social network sites or the internet is not allowed. As written in our using digital images policy.

- Only school equipment will be used for taking photographs of children which can only be used for school purposes. All images must not be stored on mobile devices but securely on the schools shared server where password access protects the images.

4.4 Communication technologies

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

Email:
All staff and children have a secure Gmail e mail address. This is the only e mail they access in school or using school ICT hardware. Only official email addresses should be used to contact staff/pupils.
The North Tyneside Grid for learning filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts. 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.

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. All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy. All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. All NTLP e mails contain the disclaimer.

Social Networks:

Many adults and pupils regularly use Social Network sites, e.g. Facebook or Twitter, although the minimum age for registering for some of these excludes primary school pupils. These communication tools are, by default, 'blocked' through the internet filtering system for direct use in North Tyneside schools. However, comments made outside school on these sites may contravene confidentiality or bring the school or staff into disrepute.

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

Although we do not allow access to social networking sites in school for children, we do understand they may use these out of school. We teach children that some sites have age restrictions for membership (eg face book age 13yr +) as well as the risks around using these sites and how to use them appropriately. Issues that relate to social networking sites such as keeping personal information safe and protecting their on line identity are taught through our e safety curriculum at appropriate times throughout the year.

Twitter and blogging may be accessed through school networks by staff through the appropriate school accounts where the use is solely for school purpose.

All staff need to be aware of the following points:
They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
If a Social Network site is used, details must not be shared with pupils and privacy settings be set at maximum. Any information recorded on a social networking site
Pupils must not be added as, 'friends' on any Social Network site.

Mobile telephone:

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

Only Yr 5 & 6 children are allowed to bring mobile phones into school if they walk to and from school unaccompanied. All mobile phones are turned off, brought to the office at 8.55 and, locked away until 3.30pm when they are collected by the children. We acknowledge that some children have phones where they can access the internet and we ensure that appropriate teaching and learning around the safety of using these devices to keep them selves safe .

Staff and visitors may bring mobile phones to school but these devices must not be used between 8.45 and 12pm and 1pm – 3.45pm and must be kept in a secure place out of view of the children and not be used in the vicinity of children. Mobiles should be switched to silent. Staff must not use mobile phones to take any photographs of children. The only exception to the use of staff mobile phones is whilst on a school trip. These devices may only be used in cases of emergency contact – school or emergency services.

Instant Messaging:

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

Children can instant messaging service when a forum or chat is set up by a teacher but this is monitored weekly by the class teachers. Any instances of inappropriate use are recorded and dealt with in line with the AUP or in instances of bullying via our school's behaviour for learning policy

Virtual Learning Environment (VLE) / Learning Platform:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Virtual Learning Environments:

- All children have logins for the Gmail. Where passwords are supplied children are taught to keep these private for security reasons. All children have Gmail e mail addresses. Pupils may only use approved e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Clear displays identify e safety and the systems and procedures to follow. These are used in whole class teaching sessions.
- As children leave the school their accounts at Monkhouse are deleted by school technician
- Internet use and spot checks is monitored on a bi-weekly basis by the school technician

Web sites and other online publications

In our school the following statements outline what we consider to be acceptable and unacceptable use of Websites and other online publications:

The NTLP page always carries an e safety section which is updated as appropriate. Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Work can only be published with the permission of the pupil and parents.

All teaching staff can edit their page on the web site and have responsibility for what appears here. The e safety champions have overall responsibility for what appears on the complete school web site.

All documentation must be in a PDF format so it cannot be altered.

Video Conferencing

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

Video chat (between users) is available through NTLP Gmail, using the video chat facility and a webcam. Other free video conferencing software (such as Skype) is easily available. It can be a wonderful way to bring the outside into the classroom and establish links with schools or individuals in other places that might not be otherwise accessible for the children's learning.

Any use of video conferencing/video chats **must only take place with the permission of an adult (see section 3)**. Any use of external video conferencing software must **not** be done with a teacher's 'personal' account. It is good practice to create a separate account for school communications. An adult must always

be present in the room when any video conferences/chats are taking place. The regulations for using webcams are similar to those for CCTV. This means that the area in which you are using the webcam must be well signposted and people must know the webcam is there before they enter the area, in order to consent being viewed in this way. Children should be consulted and adults would need to consent as well as the parents of all children involved.

In gaining consent, you must tell the person why the webcam is there, what you will use the images for, who might what to look at the images and what security measures are in place to protect access.

As children also have access to NTLP Google video chat outside of school, they must also be educated about safe, appropriate and acceptable use of these technologies, considering the following points:

- How, when and why they make use of it
- Ensuring an appropriate adult knows they are using it
- Never accepting a chat request from someone they do not know
- Reporting anything they find upsetting or inappropriate in a video chat to a trusted adult or by clicking the 'Report abuse' button on the NTLP main banner.
- Protecting their personal information when using it. This may include not just what they *say* in a 'chat', but even the objects in the room around them which may inadvertently give away personal information they don't wish to share.

Others:
As our school risk assesses and introduces new technologies we will update our policy to reflect what is considered to be acceptable and unacceptable use of these.

4.5 Acceptable Use Policy (AUP)

All staff must read and sign the 'Staff AUP' before using any school ICT resource.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

Supply staff and Visitors will be asked to read and sign the supply and visitors AUP whilst working in school.

Children and Parents will be asked to read, sign and return an AUP consent form.

The purpose of the AUP's at Monkhouse :-

- Understood by the each individual user and relevant to their setting and purpose.
- Regularly reviewed and updated.
- Regularly communicated to all users, particularly when changes are made to the eSafety Policy/AUP.
- Outlining acceptable and unacceptable behaviour when using technologies, for
- example:
    - Cyberbullying
    - Inappropriate use of email, communication technologies and Social Network sites and any online content.
    - Acceptable behaviour when using school equipment /accessing the school network.
    - 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 consequences for unacceptable use and make all users aware of the consequences (linked to the Behaviour for Learning 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.

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored.
- E safety teaching will be built into curriculum planning and policies. **Staff and the e-Safety policy**
- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school website.

4.6 Dealing with incidents

See APPENDIX 1 – Responding to eSafety Incident/ Escalation Procedures

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 1). 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
Some examples of inappropriate incidents are listed below with suggested consequences.

Incident	Procedure and Consequences
Accidental access to inappropriate materials.	Minimise the webpage/turn the monitor off. Tell a trusted adult. Enter the details in the Incident Log and report to e safety champions for 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. Be aware that a CP concern may be raised for a child if inappropriate. See CP designated teacher for any historical / current concerns.
Deliberate searching for inappropriate materials.	
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate way.	

The incidences should be logged in the incident book located in the ICT suite. (See Appendix 2)The e safety champions will check this weekly. The procedures for dealing with incidents are displayed in the ICT suite. Contact with parents will depend on the inappropriate use. Any repeat offence will involve immediate contact with parents unless it is a matter of CP which may put the child at risk of further harm.

5. Infrastructure and technology

Pupil Access:

All pupils will be supervised when accessing school equipment and on line materials.

Passwords:

All users of the school network have age appropriate username and passwords. For the gmail they have their own user name and password. The HT, SBM and LA technician are the appropriate administrators. All passwords are kept in a secure place in the office. Passwords should be changed annually.

Software/hardware:
All software has been purchased by the school and is the legal owner. The dates of appropriate licenses are recorded and kept with the secure passwords in the office. An annual audit of resources is recommended. Software/hardware. The LA technician loads any new software onto the schools network.
All staff should use an encrypted pen / removable storage device, School laps tops are for school use only and for family use or home internet access.

Managing the network and technical support:

The server and cabling is securely located and it's physical access is restricted. The net work is managed by the LA via an annual SLA. All staff should log off or lock a computer when they leave a computer / digital device unattended. A central request file is updated for LA technical support. The network is monitored via the council.

Filtering and virus protection:

Annual virus protection is purchased for the network and all school lap tops. The filtering system is done via the LA SLA. Staff have all had training for blocking / unblocking specific websites.

6. Education and Training

In 21st Century society, staff and pupils need to be digitally literate and aware of the benefits that the use of technology can provide. However, it is essential that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond.

The three main areas of eSafety risk that your school needs to be aware of and consider are:

Area of risk	Examples of risk
Commerce: Pupils need to be taught to identify potential risks when using commercial sites.	Advertising e.g. SPAM Privacy of information (data protection, identity fraud, scams, phishing) Invasive software e.g. Viruses, Trojans, Spyware Premium Rate services Online gambling
Content: Pupils need to be taught that not all content is appropriate or from a reliable source.	Illegal materials Inaccurate/bias materials Inappropriate materials Copyright and plagiarism User-generated content e.g. YouTube, Flickr, Cyber-tattoo, Sexting
Contact: Pupils 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 Contact Inappropriate emails/instant messaging/blogging Encouraging inappropriate contact

6.1eSafety across the curriculum

It is vital that pupils are taught how to take a responsible approach to their own eSafety.
Our school provide suitable eSafety education to all pupils via the following:

- Regular, planned eSafety teaching within a range of curriculum areas
- Additional focus on eSafety during the National eSafety Awareness Week
- Children with SEN will be supported through e safety education via adult support or differentiated tasks.
- All children sign the AUP and are supported in the recognising the importance of adopting safe and responsible internet use both in and out of school. Age appropriate explanations of the data protection act are provided through e safety lessons.

The different forms of 'bullying' including cyber bullying are discussed with children as part of PSHCE sessions and where to seek help if this happens to them. The safe to learn worry box is used throughout school. E safety rules are clearly displayed where children access the internet.

6.2eSafety – Raising staff awareness

All staff receive updates on e safety and awareness raising as the e safety policy is reviewed annually. The e safety champions and LA will provide guidance or training for staff. All staff are expected to promote and model responsible use of ICT and digital resources. All new staff will have a thorough induction programme which will cover e safety and AUP.

6.3eSafety – 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).

The school newsletters and NTLP offer advice on e safety for parents. The annual national e safety awareness raising is a useful platform for informing parents and carers about e safety including the benefits and risks of using various technologies. Parents are expected to support their child in understanding the AUP and sign it accordingly. Annual parent workshops on using the NTLP will include an element of internet safety.

6.4eSafety – Raising Governors' awareness

The e safety policy is regularly reviewed and approved by the governing body.

7 Standards and inspection

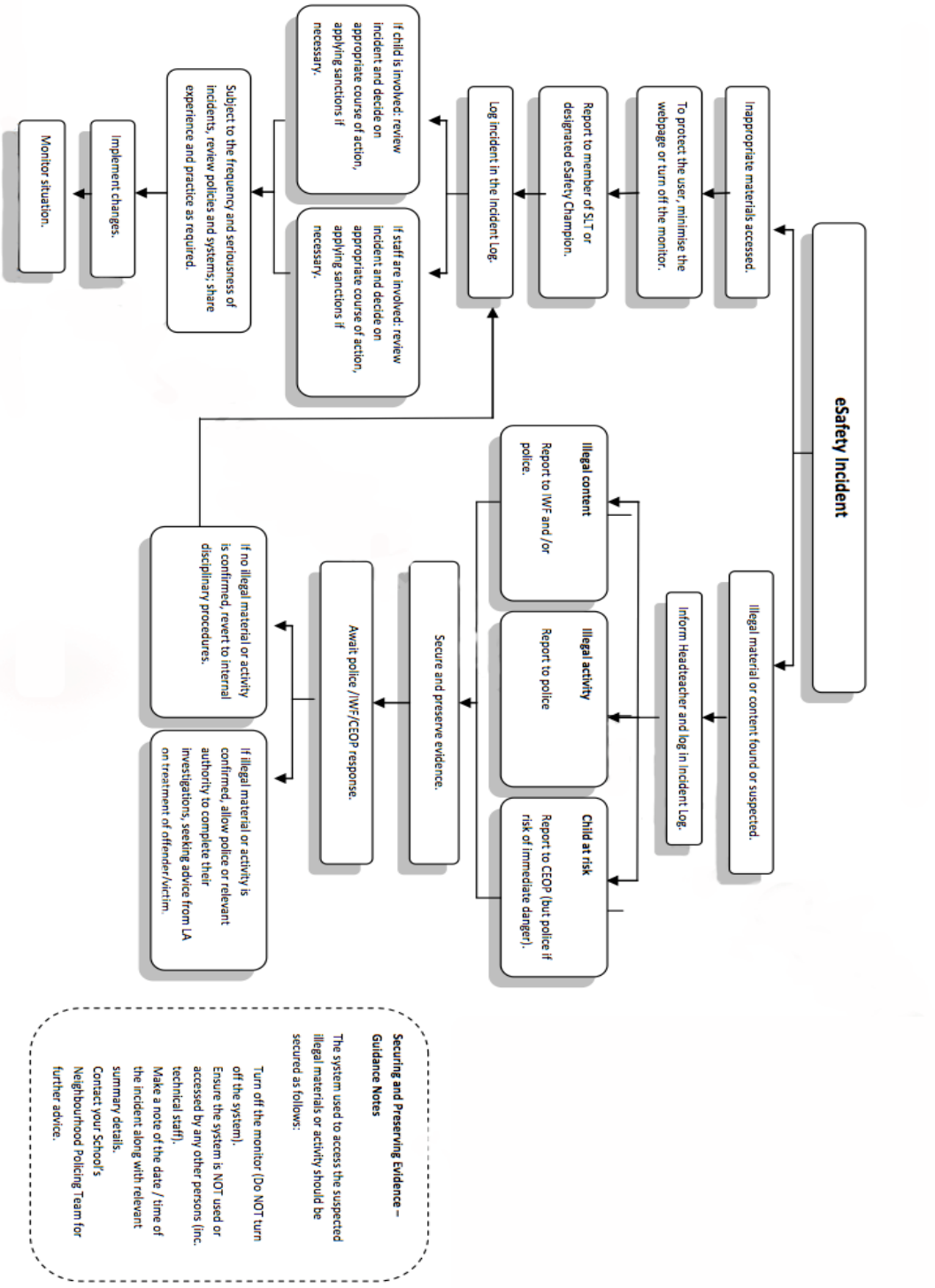
Monitoring of the incident log is completed by the e safety champions each week and they will note the numbers of inappropriate use and ensure the correct procedures have been followed. Records can be used to compare incidences historically and if any pattern emerge e.g. specific days, times, classes, groups and individual children?

APPENDIX 1 – e-Safety Incident Log

All e-Safety incidents must be recorded by the School e-Safety 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 NTLA as inappropriate.

APPENDIX 2 - Responding to eSafety Incident/ Escalation Procedures



© *Lancashire Schools' ICT Centre November 2010*