Lancashire Schools' ICT Centre

Primary Online Safety Framework Document

St Mary RC Primary School, Oswaldtwistle

Lancashire Schools' ICT Centre

2016

Developing and Reviewing this Policy

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

Kevin Egan (Compiting Subject Leader)

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

Policy Created - Date: 15th July 2015. This policy has been reviewed September 2016.

The implementation of this policy will be monitored by the Headteacher & Governors.

This policy will be reviewed as appropriate by the above named people.

Approved by ……………………………………… (Headteacher) Date ……………………………………………

Approved by ……………………………………… (Governor) Date ……………………………………………

Contents

Online Safety

Policy 2016 St Mary's RC 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 Online Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

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

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

2. Your school's vision for Online Safety

At St Mary's RC Primary School, we value the contribution that ICT can make for the benefit for all members of the school community. To this end the school uses ICT to motivate and include all pupils. All staff believe that effective use of ICT can enhance, enrich and extend learning and teaching across the curriculum.
Our vision encompasses the following aims:

To enable all members of the school community to use ICT confidently in different situations
To provide the children with the necessary skills that they can transfer into real life situations
To enable all children to become independent learners
To enable all children to use the Internet in a safe environment and to be critical and discerning with information found
To promote and to use ICT to extend and develop communication skills
To prepare all for the challenging world of changing technology

3. The role of the school’s Online Safety Champion

Our Online Safety Champion is Kevin Egan.

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

- Having operational responsibility for ensuring the development, maintenance and review of the school’s Online Safety 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 Online Safety incident occur.
- Ensuring an Online Safety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with Online Safety 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 Online Safety 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.

4. Policies and practices

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

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: 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 Online Safety Policy and statements in the Acceptable Use Policy (AUP).

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:

- The use of mobile phones by pupils is prohibited during school hours. If pupils require a mobile phone for after school activities they should leave it in an agreed secure place.
- Photographs of staff and pupils should not be taken using mobile phones by pupils or members of staff without authorisation from the Headteacher and in this even transferred to the school system as soon as practicable.

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.

Various forms of digital media offer substantial benefits to education but equally present schools with challenges particularly regarding posting or sharing media on the Internet, through mobile technologies and Social Network sites. To ensure all users are informed and educated about the risks surrounding taking, using, sharing, publishing and distributing digital media, any images taken at school will only be used for school purposes e.g. website, brochure or display.

At school photographs and video of pupils and staff are regarded as personal data in terms of The Data Protection Act (1998), and the school has written permission for their use from the individual and/or their parents or carers.

- The school seeks consent from the pupil, parent/carer or member of staff who appears in the media or whose name is used.
- The parental/carer permission is obtained in reception but the parents have a right to change this if deemed necessary.
- The staff and pupils aware that full names and personal details will not be used on any digital media, particularly in association with photographs.
- Parents/carers, who have been invited to attend school events are allowed to take videos and photographs.
- All staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites.
- The school ensures that photographs/videos are only taken using school equipment and only for school purposes
- The school ensures that any photographs/videos are only accessible to the appropriate staff/pupils.
- Staff are encouraged not to store digital content on personal equipment. The staff are encouraged not to use their own cameras.
- When taking photographs/video, staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.
- Staff, parents/carers and pupils made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved.
- The guidelines for safe practice relating to the use of digital media, as outlined in the school's policy are monitored by the S.L.T and Governors on an annual basis.

4.4 Communication technologies

School uses a variety of communication technologies and is aware of the benefits and associated risks.

Email

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

- All users have access to the Lancashire Grid for Learning service as the preferred school email system.
- Only official email addresses are used between staff and with pupils/parents when personal/sensitive data is involved.
- The Lancashire Grid for Learning filtering service reduces the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to the Westfield Centre.
- 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.
- Our school includes a standard disclaimer at the bottom of all outgoing emails (see below).

St Mary's school email disclaimer:

****

This e-mail is confidential and privileged. If you are not the intended
recipient do not disclose, copy or distribute information in this e-mail
or take any action in reliance on its content.

****

****

This email has been checked for known viruses.

Social Networks:

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

Social Network sites allow users to be part of a virtual community. Current popular examples of these are Facebook, Twitter, Bebo and Club Penguin. These sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a Social Network site, you may have access to view other users' content, send messages and leave comments.

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.
- Pupils must not be added as 'friends' on any Social Network site.
- Children who are under 13 are not legally allowed to members of Facebook.

Remember; whatever means of communication you use you should always conduct yourself in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever.

Mobile telephone:

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

- The school allows personal mobile phones to be used in school by staff and visitors but are

asked to be left on silent in curriculum time.

- It is acceptable to use personal mobile phones for school activities e.g. school trips.

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:

School has chosen to use Purple Mash as a communication tool.

- All children will be given access to the Purple Mash but SLT have access to all accounts.
- Passwords are issued to the children and they are encouraged not to share their password.
- Pupils are taught to use these communication tools in a responsible way in conjunction with the Online Safety curriculum.
- Teachers know how to monitor the use of the Moodle with their class.
- Accounts are deleted when staff and pupils leave the school. This is monitored by the SLT.

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:

This may include for example, podcasts, videos, 'Making the News' and blogs.

- The school website is effective in communicating Online Safety messages to parents/carers.
- Everybody in the school is made aware of the guidance for the use of digital media on the website.
- Everybody in the school aware of the guidance regarding personal information on the website.
- Teachers have access to edit the school website.
- The Head teacher has overall responsibility for what appears on the website.

Others:
The School will adapt/update the Online Safety policy in light of emerging new technologies and any issues
or risks associated with these technologies.

4.5 Acceptable Use Policy (AUP)

Use of ICT for educational, personal and recreational purposes.

AUPs (see appendix 2,3,4 & 5) are used for Staff and pupils and must be signed and adhered to by users before access to technology is allowed. This agreement is as a partnership between parents/carers, pupils and the school to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology is kept in school and made available to all staff.

Our school AUPS aim to:

- Be understood by the each individual user and relevant to their setting and purpose.
- Be regularly reviewed and updated.
- Be regularly communicated to all users, particularly when changes are made to the Online Safety Policy/AUP.
- Outline 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 sanctions for unacceptable use and make all users aware of the sanctions (linked to our Behaviour Policy).
- Stress the importance of Online Safety education and its practical implementation.
- Highlight the importance of parents/carers reading and discussing the content of the AUP with their child.

4.6 Dealing with incidents

Here are the types of incident that may occur and how these will be dealt with in our school.
An incident log will need to be completed to record and monitor offences(see appendix 1) . This will be auditedon a regular basis by the Computing Subject Leader 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, LCC Safeguarding,CEOP, Internet Watch Foundation (IWF). **No staff member will ever personally investigate, interfere with or share evidence as they may inadvertently be committing an illegal offence.** It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident-

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 our 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. Examples of inappropriate incidents are listed below with suggested sanctions for our school.

Incident	Procedures and Sanctions
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 LGfL filtering services if necessary. Persistent 'accidental' offenders may need further disciplinary action.
Using other people's logins and passwords maliciously.	Using other people's logins and passwords maliciously. Inform SLT or designated e-Safety Champion. Enter the details in the Incident Log. Additional awareness raising of Deliberate searching for inappropriate materials.
Bringing inappropriate electronic files from home.	e-Safety 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, for specific or repeated non-accidental incidents.

Procedures when dealing with E-Safety;
- Responsible persons – Headteacher, E-Safety Champion.
- All staff made aware of our procedures to recognise and deal with E-safety incidents (see appendix 9)

- Responding to safety incidents will be displayed in Staffroom and ICT Suite as a guidance
- Children are given e-safety guidance as part of curriculum each term
- Incidents will be logged on Form Appendix 1 in file in ICT Suite and monitored by E-Safety Champion

• Review of policy/procedures in line with frequency and seriousness of incidents.

Infrastructure and technology

The school ensures that the infrastructure/network is as safe and secure as possible. Broadband connection, filtering and virus protection are provided (by default) by the Lancashire Grid for Learning.

Pupil Access:

- The children are supervised by staff when accessing school equipment and online materials

Passwords:

- All staff aware of the guidelines in the Lancashire ICT Security Framework for Schools. This is available at www.lancsngfl.ac.uk/ Online Safety website.
- All users of the school network have a secure username and password.
- The administrator password for the school network available to the Headteacher and other nominated senior leader is kept in a secure place.
- Staff and pupils are reminded of the importance of keeping passwords secure
- Passwords will only be changed if the need arises.

Software/hardware:

- The school has legal ownership of all software.
- The school has an up to date record of appropriate licences for all software and the ICT co-ordinator is responsible for maintaining this.

Managing the network and technical support:

- Servers, wireless systems and cabling are securely located and physical access restricted.
- The SLT is responsible for managing the security of the school network.
- The safety and security of the school network Is monitored on a regular basis.
- The school systems are kept up to date in terms of security e.g computers are regularly updated with critical software updates/patches.
- Users (staff, pupils, guests) have clearly defined access rights to the school network e.g. they have a username and password.
- Staff and pupils are encouraged to lock or log out of a school system when a computer/digital device is left unattended.
- Only the administrator is allowed to download executable files and install software.

- Users report any suspicion or evidence of a breach of security to the SLT
- The school encourages staff not to use removable storage devices on school equipment e.g. encrypted pen drives.
- The school encourages teachers to follow e-safety policy guidelines when using laptop for personal/family use
- If network monitoring takes place, it is in accordance with the Data Protection Act (1998)
- All internal/external technical support providers are aware of your schools requirements / standards regarding Online Safety
- The SLT is responsible for liaising with/managing the technical support staff.

6. Education and Training

In 21st Century society, pupils need to be digitally literate and aware of the benefits that 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.

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. Virus', Trojans, Spyware Premium Rate services Online gambling.
Content: Pupils need to be taught that not all content is appropriate or from a reliable source.	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 Online Safety. St Mary's provides suitable Online Safety education to all pupils:

- Regular, planned Online Safety teaching within a range of curriculum areas (using the Lancashire ICT Progression framework)
- E-Safety education is differentiated for pupils with special educational needs.
- Pupils are made aware of the impact of Cyberbullying and how to seek help if they are affected by these issues, e.g. using peer mentoring.
- Pupils are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.
- The school ensures that pupils 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.
- Pupils are reminded of safe Internet use e.g. classroom displays, Online Safety rules (See

Appendices), acceptance of site policies when logging onto the school network /Purple Mash

6.2eSafety – Raising staff awareness

There is a programme of formal Online Safety training for all staff to ensure they are regularly updated on their responsibilities as outlined in our school policy.

- The Online Safety co-ordinator provides advice/guidance or training to individuals as and when required.
- The Online Safety training ensures staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites.
- All staff are expected to promote and model responsible use of ICT and digital resources.
- Online Safety training is provided within an induction programme for all new staff to ensure that

they fully understand both the school's Online Safety Policy and Acceptable Use Policy.

- Regular updates on Online Safety Policy, Acceptable Use Policy, curriculum resources and general Online Safety issues are discussed in staff/team meetings.

6.3eSafety – Raising parents/carers awareness

The school offers opportunities for parents/carers and the wider community (appendix 8) to be informed about
Online Safety including the benefits and risks of using various technologies. For example through:

- School newsletters, Website and other publications.
- Promotion of external eSafety resources/online materials.

6.4eSafety – Raising Governors' awareness

The school considers how Governors, particularly those with specific responsibilities for Online Safety ICTor child protection, are kept up to date. This is through discussion at Governor meetings, attendance at Local Authority Training, CEOP or internal staff/parent meetings.
NB The Online Safety Policy will be reviewed yearly (and/or if a serious breach occurs) by the Online Safety
coordinator, approved by the governing body and made available on the school's website.

7 Standards and inspection

Since January 2014 there has been greater emphasis on monitoring safeguarding procedures throughout schools.
At St Mary's:

- E-Safety incidents are monitored, recorded and reviewed.
- The SLT are responsible for monitoring, recording and reviewing incidents.
- The introduction of new technologies is risk assessed.
- These assessments are included in the Online Safety Policy.
- Incidents are analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children.
- These patterns would be addressed most effectively by e.g. working with a specific group, class assemblies, reminders for parents.

APPENDIX 1

St Mary’s RC Primary School Online Safety Incident Log

Details of ALL Online Safety incidents to be recorded by the Online Safety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying may also need to be recorded elsewhere

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

APPENDIX 2

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 Online Safety 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 Online Safety 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 *Mr Egan.*

Yours sincerely,

Appendix 3

St Mary's RC Primary School ICT Acceptable Use Policy (AUP) - Children

These rules reflect the content of our school's Online Safety 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 Online Safety
- 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 *St Mary's RC Primary School*
.
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 4

St Mary's RC Primary School 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 Online Safety 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 Kevin Egan/John Kavanagh.

10. I will ensure that personal data (including data held on MIS systems) is kept secure at all timesand 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 Online Safety 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

St Mary’s RC Primary ICT Acceptable Use Policy (AUP) – Students, Supply Teachers, Visitors, Guests.

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

Our Golden Rules for Staying Safe with ICT (KS1)

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 7

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

Appendix 8

Example of Letter to Parents Regarding Parental Online Safety 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 Online Safety 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,

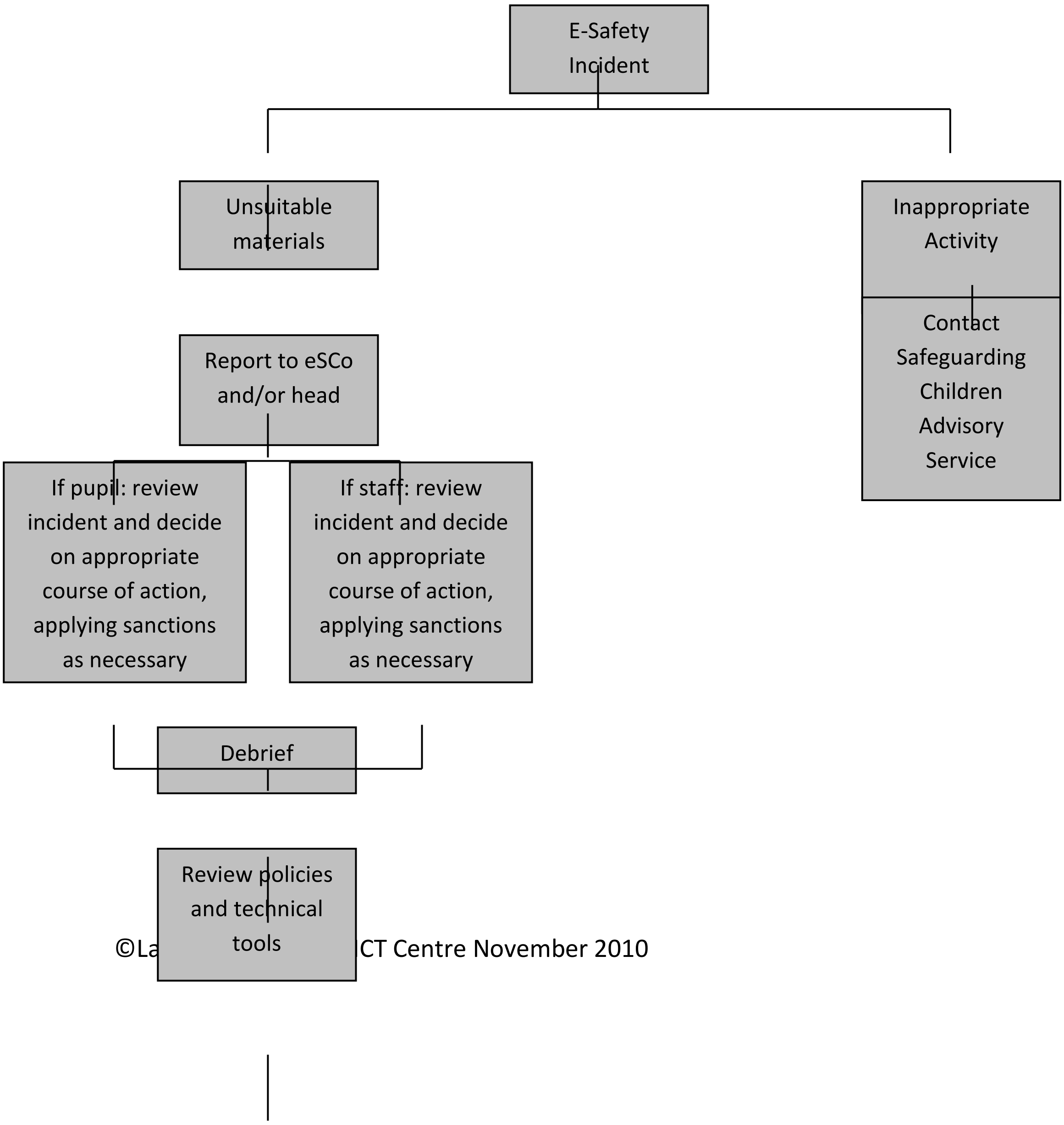
<The Headteacher>

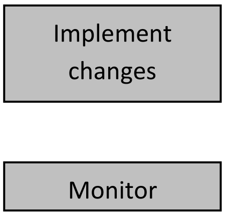
I / we will be attending the above Parental eSafety Awareness Session

Name(s):...

Appendix 9

Flowchart for responding to e-safety incidents in school


E-Safety Incident
Unsuitable materials
Inappropriate Activity
Contact Safeguarding Children Advisory Service
Report to eSCo and/or head
If pupil: review incident and decide on appropriate course of action, applying sanctions as necessary
If staff: review incident and decide on appropriate course of action, applying sanctions as necessary
Debrief
Review policies and technical tools



Implement changes

Monitor