

St Mary's RC Primary
School, Swinton,
Manchester
E-Safety Policy

January 2010
Mrs L Croston
Miss J. Dixon

Index

| | |
|----------------------------------------------------|----|
| 1.0 What is E-Safety? | 4 |
| 1.1 Introduction | 4 |
| 1.2 Roles and Responsibilities | 5 |
| 1.2.1 E-Safety skills development for staff | 5 |
| 1.2.2 Managing the schools E-Safety message | 5 |
| 2.0 E-Safety in the Curriculum | 6 |
| 2.1 Password Security | 6 |
| 2.2 Managing E-Safety within school | 7 |
| 2.2.1 Infrastructure | 7 |
| 2.3 Managing E-Safety outside of school | 8 |
| 2.3.1 Pupils, Parents and Carers | 8 |
| 2.3.2 Schools Staff | 8 |
| 3.0 Mobile Technologies | 9 |
| 3.0.1 Pupil mobile devices | 9 |
| 3.0.2 Staff mobile devices | 9 |
| 3.0.3 School provided mobile devices | 9 |
| 3.1 Managing email | 10 |
| 3.2 Safe Use of Images | 10 |
| 3.2.0 Publishing pupils images and work | 11 |
| 3.2.1 Storage of images | 11 |
| 3.3 Data security | 11 |
| 3.4 Copyright | 12 |
| 3.5 Portable and removable storage devices | 12 |
| 3.5.1 Purpose | 13 |
| 3.5.2 Acceptable usage | 13 |
| 3.5.3 User responsibilities | 13 |
| 3.5.4 Use of USB storage devices | 14 |
| 4.0 Child Protection | 14 |
| 4.1 Cyber Bullying guidance | 15 |
| 4.2 Misuse and Infringements | 16 |

| | |
|----------------------------------------------|----|
| 4.2.1 Complaints | 16 |
| 4.2.2 Inappropriate material | 16 |
| 5.0 Equal Opportunities | 17 |
| 6.0 Writing and reviewing this Policy | 17 |
| 7.0 Staff E-Safety incident flowchart | 18 |
| 7.1 Pupil E-Safety incident flowchart | 19 |

What is E-Safety?

Protecting young people properly means thinking beyond the traditional school environment. Where once the desktop computer was the only way to access the internet now many mobile phones and games consoles offer broadband connections.

Pupils may be working online in school, at home or in an internet cafe. They may have personal devices not covered by network protection and therefore the emphasis should be on getting everyone to understand the risks and act accordingly.

The Internet has become an integral part of pupil's lives, enabling them to undertake research for school projects, talk to their friends and access information from around the world. Increasing provision of the Internet in and out of schools brings with it the need to ensure that learners are safe.

Internet development is constantly evolving into ever more innovative areas, with many websites enabling amazing creativity and interaction between peers.

Unfortunately though, there are times when Internet use can have a negative effect on children. Pupils, staff, parents and carers should be aware of the potential dangers and take measures to ensure safe usage of technology.

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile / Smart phones with text, video and / or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At St Mary's we understand the responsibility to educate our pupils on E-Safety issues, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies in, and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement are inclusive of both fixed and mobile internet technologies provided by the school (such as PC's, laptops, personal digital assistants (PDAs), tablet PC's, webcams, whiteboards, voting systems, digital video equipment, digital cameras, visualisers etc); and technologies owned by pupils and staff brought onto school premises such as laptops, mobile phones etc.

Roles and Responsibilities

As E-Safety is an important aspect of strategic leadership within the school, the Head Teacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. Mrs Croston has been designated the role of E-Safety Co-ordinator within the school. All members of the school community have been made aware of who holds this post. It is the role of the E-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Salford LA, BECTa, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Director of ICT and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's Acceptable Use Policy for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community.

E-Safety skills development for staff

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community. (See section 7.0 & 7.1)
- All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas.

Managing the school E-Safety message

- The E-Safety rules will be reinforced to the pupils at the start of each school year as part of the SEAL scheme of work.
- E-Safety posters will be prominently displayed in the ICT room including the pupil e-safety incident flow chart.

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety.

- Educating pupils on the dangers of technologies that maybe encountered outside school is done through the ICT curriculum will be covered by other curriculum areas where appropriate.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent / carer, teacher / trusted staff member, or an organisation such as Childline / CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

Password Security

Password security is essential for pupils and staff, particularly for staff as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's E-Safety Policy.
- Users are provided with an individual network log-in from year 3 and they are also expected to use a personal password and keep it private.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to Mrs Croston.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and data, MIS systems and / or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- Staff are advised to update their passwords every 6 months or sooner if they think someone else knows their password.
- Under no circumstances are staff allowed to let any other person to use their user name and password (This could result in disciplinary action).

Managing E-Safety within school

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- The school maintains pupils will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites and materials before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- At present, the school endeavours to deny access to social networking sites to pupils within school and promotes the Radiowaves website as a safe, monitored environment by which pupils can communicate in a similar way to social networking sites.

Infrastructure

- Salford Local Authority has a monitoring solution where web-based activity is monitored and recorded.
- School internet access is controlled through the LAs web filtering service.
- St Mary's is aware of its responsibility when monitoring staff communication under current legislation and takes into account the Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000 and Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off / closed and the incident reported immediately to the class teacher.
- Pupils and staff are not permitted to download programs or files.

Managing E-Safety outside of school

Web technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

Pupils, Parents and Carers

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils, parents and carers are advised to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the

appropriateness of any images they post due to the difficulty of removing an image once online.

- Pupils, parents and carers are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile / home phone numbers, school details, IM / email address, specific hobbies / interests).
- Pupils, parents and carers are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils, parents and carers are asked to report any incidents of bullying to the school.
- The school advises parents and carers to locate PC's and laptops in a highly visible part of the home, which can be regularly monitored.
- Pupils should not meet anyone that they have met through the internet, unless accompanied by a trusted adult.

School Staff

- If you are a member of a social networking (e.g. Face book) ensure that you security settings are high. If you need further advice on this matter see the ICT Co-ordinator.
- Staff on social networking sites are advised not to accept past and current pupils as friends.
- Staff are advised to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- School laptops are only to be used by the staff member allocated the laptop. The laptop should not be used by family members and should only be used for work purposes not personal use.
- Under no circumstances are staff to take offsite any images and videos taken within the school environment without the authorisation of the Head Teacher.

Mobile technologies (Including mobile phones)

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Pupil Mobile devices

- Pupils are only allowed to bring personal mobile devices/phones to school with prior permission from their class teacher and then they will only be allowed to bring personal mobile devices / phones to school if they follow the following: they must not use them for personal purposes during the school day. At all times the device must be switched onto silent.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Staff Mobile devices

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent or carer using their personal device **unless in the use of an emergency.**
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices

- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as laptops and PDAs for offsite visits and trips, only these devices should be used.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving emails.

At St Mary's:

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged and if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents / carers or conduct any school business using personal email addresses.
- Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Pupils must immediately tell a teacher / trusted adult if they receive an offensive email.
- Staff must inform the E-Safety co-ordinator / line manager if they receive an offensive email.
- Pupils are introduced to email as part of the ICT Scheme of Work in Year 3.

Safe Use of Images and Film

Digital images are easy to capture, reproduce and publish and therefore misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

At St Mary's:

- With the written consent of parents (on behalf of pupil's), the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment such as mobile phones and cameras to record images of pupils unless they have prior authorisation from the Headteacher. This includes when on trips.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras to record images of the pupils or staff within the school environment or when on trips, unless prior consent has been given by the Headteacher; e.g. for residential trips and then this would only be allowed under close supervision by the staff present and while the staff were present. Cameras would then be stored e.g. overnight by the staff, to prevent the misuse of them. Under no circumstances should children have access to cameras, or any other picture taking device, where others may be in a state of undress e.g. a dormitory.

Publishing pupil's images and work

On a child's entry to the school, all parents / carers will be asked to give permission to use their child's work / photos in the following ways:

- On the school web site.
- In the school prospectus and other printed publications that the school may produce for promotional purposes.
- In display material that may be used in the school's communal areas.
- General media appearances. e.g. local / national press to highlighting an activity. (Sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue. e.g. divorce of parents, custody issues etc.

Parents / carers may withdraw permission in writing at any time.

Email and postal addresses of pupils will not be published.

Only the Web Manager has authority to upload to the school's website.

Storage of Images

At St Mary's:

- Images / films of children are stored on the school's network.

- Pupils and staff are not permitted to use personal portable media for storage of images without the express permission of the Head Teacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

At St Mary's:

- Staff are aware of their responsibility when accessing school data. Level of access is determined by the Head Teacher and implemented by the ICT co-ordinator.
- Any data taken off the school premises must be encrypted. (Advice must be sought from the ICT Network Manager when doing this).
- Data can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any school, children or pupil data.

Copyright

The infringement of copyright is a criminal offence under the Copyright, Designs and Patents Act 1988 and could result in prosecution.

Just because something is on the web does not mean it is freely available for you to use in your own work.

As with any material which is protected by copyright, you should seek the author's permission if you wish to use it.

With text you can use up to 5% of any one piece of work without seeking permission.

With images, sound, animations, and video clips, you should seek permission, unless you are specifically told you can download and use them freely.

Copyright law allows students special concessions but these are very limited. As a member of staff or a student you may use copyright material for your own personal study purposes only. This includes using copyright material as part of an assignment. If you later want to use the same material for any other purpose, you must seek permission.

You should always acknowledge the source of any 'third party' material you include in your own work.

Portable & Removable Storage Devices (RSD)

Over recent years staff have increasingly needed to be fully mobile and connected, often taking information home or out of the school in order to maintain productivity and deliver services efficiently and effectively.

As a result, the use by staff of mobile portable devices such as laptops, tablet PC's, USB pen drives, PDAs, XDAs, and other mobile devices has proliferated in recent years.

In order to ensure the schools information assets are protected and used in a responsible manner, the school is adopting and implementing this Removable Storage Device (RSD) policy. This policy clearly defines the responsibilities of all staff members, supply staff, contract staff, partners and anyone who comes into direct or otherwise contact with school information via such devices.

The successful operation of this new policy cannot be achieved without the full co-operation of every information user. It is therefore imperative that any member of staff or agent reports any actual or suspected security breach within their area of activity.

Purpose

This document describes the policy for the acceptable and secure usage of Portable & Removable Storage Devices (RSD) within St Mary's. This policy is not designed to prevent the use of such devices, but rather informs users of what they can or cannot do and the consequences of not complying with the terms of this policy.

Use of such devices is permitted for authorised business purposes only.

This policy covers all mobile and removable storage devices which can be connected via a number of means and includes:

- Laptops and tablet PC's
- USB sticks / pen drives / flash drives etc.
- iPhone, ipod or Smartphone's
- XDA or PDA devices
- Memory cards e.g. compact flash, Secure Digital (SD), XD
- PC Card / PCI / PCMCIA
- Cameras with a USB (or other) drive connection
- Other data storage devices e.g. CD-ROM, DVD, external hard drives
- Bluetooth
- Wi-Fi
- Infra Red (IR)

Acceptable Usage

Portable devices such as laptops / tablet PCs, DVDs, CDs and in particular USB-based pen drives are highly convenient tools in the modern workplace for storage of information and data. Their storage capacity, portability, low price and plug-and-play functionality is some of the reasons why their use has increased enormously within the school. However, it is their portability that can potentially expose the member of staff and the school to additional risk should sensitive information stored on them fall into the wrong hands.

User responsibilities

Users are responsible for:

- The security of any RSD devices in their possession.
- The data stored on an RSD being transported is encrypted.
- RSDs must not be used to bring unauthorised data or malicious code onto the school network.
- An RSD should not be used to copy / transport data without appropriate permission.
- RSDs must not be used in a way that contravenes any legislation e.g. Data Protection Act.

- Any loss or suspected loss of an RSD that contains data that is protectively marked, personal or could cause the school to suffer financial loss or reputational damage.

Use of USB storage devices

Staff should seriously consider whether the use of a USB pen drive is entirely appropriate. Often they are used purely to store data to enable staff to be able to work from home. If access to work related data is needed at home you must first seek advice from the ICT co-ordinator.

Where USB pen drives are to be used to store and transport child related data, only pre-approved storage media are to be used. This media should be encrypted and biometrically secured. When transporting data of this nature you must always first seek advice from the ICT co-ordinator and gain prior approval from the E-Safety Coordinator.

The use of personally owned storage media (i.e. non ICT Services supplied) or software only encrypted USB pen drives is NOT PERMITTED for the storage of such data.

Child Protection

Although the use of ICT and the internet provide ever increasing opportunities for children to expand their knowledge and skills, it is also the case that the use of such technology may sometimes expose children to risk of harm.

Apart from the risk of children accessing internet sites which contain unsuitable material, risks to the well being of children may also exist in a variety of other ways.

It is known that adults who wish to abuse children may pose as children to engage and then meet up with the young people they have been in communication with.

This process is known as 'Grooming' whereby an adult prepares a child or young person to be abused. The process may take place over a period of months using chat rooms, social networking sites and mobile phones.

An adult may pretend to be a peer and gradually convince the child or young person that they are their boyfriend or girlfriend, establishing a relationship of apparent trust with the intended victim and making it difficult for the child to then speak out.

Increasingly bullying is conducted on the internet or by the use of text messages and is therefore harder for schools to notice and deal with.

As with all forms of harm or abuse, there is no exhaustive list of signs or indicators to watch out for. But these can include: changes in children's behaviour, demeanour, physical appearance and presentation, language or progress.

If you are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child:

1. Report to and discuss with Mrs Croston E-safety co-ordinator in school.
2. Advise the child on how to terminate the communication and attempt to save all evidence.

3. Contact Child Exploitation and Online Protection centre (CEOP) at www.ceop.gov.uk
4. Consider the involvement of police and social services.
5. Consider informing the Local Authority E-Safety officer Lesley Craven.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

Cyber bullying Guidance

Cyber bullying is bullying through the use of communication technology like mobile phone text messages, emails or websites.

This can take many forms for example:

- Sending threatening or abusive text messages or emails, personally or anonymously.
- Making insulting comments about someone on a website, social networking site (e.g. MySpace) or online diary (blog).
- Making or sharing derogatory or embarrassing videos of someone via mobile phone or email.

Abusive language or images used to bully, harass, threaten another, whether spoken or written (through electronic means) may be libellous and may contravene the Harassment Act 1997 or the Telecommunications Act 1984.

Within our Anti-Bullying Policy, Behaviour policy and Acceptable Use Agreement the use of the web, text messages, email, video or audio to bully another pupil or member of staff will not be tolerated. Bullying can be done verbally, in writing or images, including through communication technology (cyber bullying) e.g. graffiti, text messaging, email or postings on websites. It can be done physically, financially (including damage to property) or through social isolation.

Children and staff should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

If a bullying incident directed at a child or member of staff occurs using email or mobile phone technology either inside or outside of school time

- Advise the child / staff member not to respond to the message.
- Refer to relevant policies including E-Safety Policy, Acceptable Use Agreement, Anti-bullying policy and apply appropriate sanctions.
- Secure and preserve any evidence.
- Inform the sender's email service provider.
- Notify parents of the children involved or in the case of a member of staff follow the incident reporting flowchart.
- Consider informing the police depending on the severity or repetitious nature of offence.
- Consider Informing the Head Teacher and LA E-Safety officer (Lesley Craven) depending on the severity.

If malicious or threatening comments are posted on an Internet site about a pupil or member of staff

- Inform and request the comments be removed if the site is administered externally.
- Secure and preserve any evidence.
- Send all the evidence to appropriate point of contact via the E-Safety incident flowchart.
- Endeavour to trace the origin and inform police as appropriate.
- Consider informing the Head Teacher or LA E-Safety officer (Lesley Craven).

Misuse and Infringements

Any misuse of computer equipment or mobile technology that breaches any of the guidelines set out in the E-Safety policy should be reported to the E-Safety co-ordinator.

Should an infringement of the schools Acceptable Use Agreement, E-Safety Policy or Removal Storage Device Policy occur, it should be reported to the E-Safety co-ordinator, Mrs Croston.

Complaints

Complaints relating to E-Safety should be made to Mrs Croston, E-Safety Coordinator or the Head teacher at the following address:

St Mary's
 Milner Street
 Swinton
 Manchester
 M27 4AS
 0161 794 4028

Inappropriate material

At St Mary's:

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported and follow E-Safety incident flowchart.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the teacher or Mrs Croston, E-Safety Coordinator depending on the seriousness of the offence.
- Serious infringements may result in investigation by the Head Teacher / LA and could lead to immediate suspension, possibly leading to dismissal and involvement of police.

Equal Opportunities

The school endeavours to create a consistent message with parents and carers for all pupils and this in turn should aid establishment and future development of the schools' E-Safety policy.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well managed for these children and young people.

Writing and Reviewing this Policy

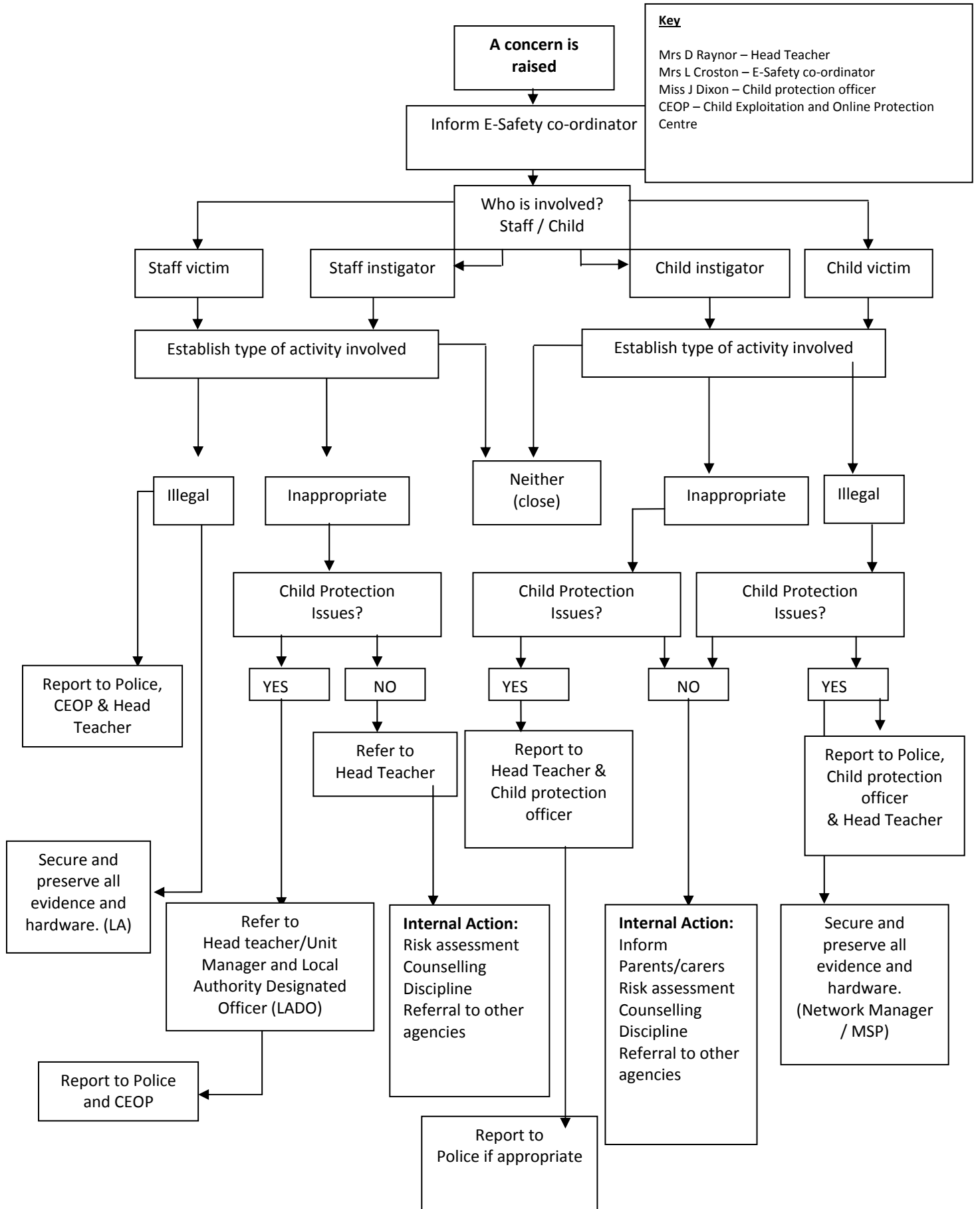
There will be an on-going opportunity for staff and parents to discuss with the school and E-Safety co-ordinator any issue of E-Safety that concerns them.

This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning.

The governors agreed this policy on(date) and it will be reviewed in partnership with staff, parents / carers and students again on(date) unless there are changes in National or Local Guidance

Signed _____

St Mary's Staff E-Safety incident flowchart



St Mary's Pupil E-Safety incident flowchart

You have a concern about something you've seen on a computer.

At home

Tell a parent / carer or trusted adult

Inform school, police or CEOP as appropriate

At school

Turn off your monitor but not your PC

Calmly and quietly put your hand up. Without discussing the incident with anyone else inform the class teacher

Teacher to refer to E-Safety flowchart



CEOP = Child Exploitation and Online Protection
<http://www.ceop.gov.uk>