# MARTONGATE PRIMARY SCHOOL

# E safety

# POLICY

**UPDATED BY:** Gemma Petch
(SIRO board member:teacher)

**DATE:** December 2014

# CONTENTS

## Introduction

At Martongate we recognise that the Internet and other technologies have an important role in the learning and teaching process. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. There are many benefits to using the internet both inside and outside of the classroom and, as a school, we are dedicated to the use of new technologies to enhance teaching and learning. However, we also recognise that it is equally important to balance these benefits with an awareness of the potential risks. This policy will identify how issues surrounding e safety are addressed throughout our school and will also reflect our school's commitment to the safeguarding and well-being of pupils, staff and all other stakeholders.

This policy applies to the whole school community including the senior leadership team, school board of governors, all staff employed directly or indirectly by the school and all pupils.

This policy will be reviewed and updated regularly, following the safeguarding SIRO Board meetings.

## Responsibilities

We believe that e safety is the responsibility of the whole school community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute

### Responsibilities of the senior leadership team

- The headteacher is ultimately responsible for safeguarding provision (including eSafeguarding) for all members of the school community, though the day-to-day responsibility for eSafeguarding will be delegated to the eSafeguarding Leader.
- The headteacher and senior leadership team are responsible for ensuring that the eSafeguarding Leader and other relevant staff receive suitable training to enable them to carry out their eSafeguarding roles and to train other colleagues when necessary.
- The headteacher and senior leadership team will ensure that there is a mechanism in place to allow for monitoring and support of those in school who carry out the internal eSafeguarding monitoring role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.
- The senior leadership team will receive monitoring reports from the eSafeguarding Leader.
- The headteacher and senior leadership team will ensure that there is a risk management function in place within school (SIRO Board) and that this function is managed, taken seriously and formalised.
- The headteacher and senior leadership team should receive update and progress reports from the SIRO Board.
- The headteacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious eSafeguarding incident.

- The headteacher and senior leadership team will ensure that all members of staff receive an appropriate level of training in eSafeguarding issues.
- The headteacher and the senior leadership team will ensure that all stakeholders within school and third party contractors or visitors will be made aware of securing information through applicable physical or electronic controls and be made aware of the school's data-protection obligations.

Responsibilities of the eSafeguarding Leader

- To promote an awareness and commitment to eSafeguarding throughout the school.
- To be the first point of contact in school on all eSafeguarding matters.
- To take day-to-day responsibility for eSafeguarding within school and to have a leading role in establishing and reviewing the school eSafeguarding policies and procedures.
- To lead the school eSafeguarding group/SIRO board.
- To communicate regularly with school technical staff.
- To communicate regularly with the designated eSafeguarding governor.
- To communicate regularly with the senior leadership team.
- To create and maintain eSafeguarding policies and procedures.
- To develop an understanding of current eSafeguarding issues, guidance and appropriate legislation.
- To ensure that all members of staff receive an appropriate level of training in eSafeguarding issues.
- To ensure that eSafeguarding education is embedded across the curriculum.
- To ensure that eSafeguarding is promoted to parents and carers.
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.
- To monitor and report on eSafeguarding issues to the eSafeguarding SIRO Board and the senior leadership team as appropriate.
- To ensure that all staff aare aware of the procedures that need to be followed in the event of an eSafeguarding incident.
- To ensure that an eSafeguarding incident log is kept up to date.
- To work closely where appropriate with the designated Child protection coordinator
- To ensure that any child protection related issues are reported to the designated child protection coordinator

Responsibilities of the eSafeguarding SIRO Board

- To ensure that the school eSafeguarding policy is current and pertinent.
- To ensure that the school eSafeguarding policy is reviewed at prearranged time intervals.
- To ensure that school Acceptable Use Policies are appropriate for the intended audience.
- To promote to all members of the school community the safe use of the internet and any technologies deployed within school.

- To risk assess all information systems, both physical and electronic for vulnerabilities and risks and recommend suitable counter measures.
- To risk assess all technology in use within school both from an administration and curriculum perspective for safe and acceptable use.
- To understand the data-protection obligations of the school along with the Data Protection Officer and understand where and how school-owned information is being processed.

Responsibilities of Teachers and Support Staff

- To read, understand and help promote the school's eSafeguarding policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Policy.
- To report any suspected misuse or problem to the eSafeguarding Leader.
- To develop and maintain an awareness of current eSafeguarding issues and guidance.
- To model safe and responsible behaviours in their own use of technology.
- To maintain a professional level of conduct in personal use of technology at all times.
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones etc.
- To embed eSafeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology.
- To ensure that pupils are fully aware of research skills and of legal issues relating to electronic content, such as copyright laws.
- To understand and be aware of incident-reporting mechanisms that exist within the school.

Responsibilities of Technical Staff

- To read, understand, contribute to and help promote the school's eSafeguarding policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Policy.
- To report any eSafeguarding-related issues that come to your attention to the eSafeguarding Leader.
- To have membership/representation on the SIRO board.
- To present technical and information-based risks to the SIRO in a non-technical understandable language.
- To develop and maintain an awareness of current eSafeguarding issues, legislation and guidance relevant to their work.
- To support the school in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the school network is only through an authorised, restricted mechanism.

- To have a basic understanding of the schools data-protection obligations and recognised information security strategies.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for the security of the school ICT systems.
- To liaise with the local authority and other appropriate people and organisations on technical issues.
- To document all technical procedures and review them for accuracy at appropriate intervals.
- To restrict all administrator level accounts appropriately.
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school.
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted.
- To be a member of the SIRO Board that meets termly to review eSafeguarding incidents that have occurred within school.
- To ensure that any use of school-owned equipment by external groups or third parties will be logged and monitored for accountability purposes.

Responsibilities of Pupils

- To read, understand and adhere to the school pupil Acceptable Use Policy.
- To help and support the school in the creation of eSafeguarding policies and practices (consultation e.g. School council and online surveys) and to adhere to any policies and practices the school creates.
- To know and understand school policies on the use of mobile phones, digital cameras and handheld devices.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely, both in school and at home.
- To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws.
- To take responsibility for each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school.
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.

- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school.
- To discuss eSafeguarding issues with family and friends in an open and honest way.

Responsibilities of Parents and Carers

- To help and support the school in promoting eSafeguarding.
- To read, understand and promote the school pupil Acceptable Use Policy with their children.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To discuss eSafeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- To model safe and responsible behaviours in their own use of technology.
- To consult with the school if they have any concerns about their children's use of technology.
- To agree to and sign the Home School Agreement which clearly sets out the use of photographic and video images outside of school.
- To sign a Home School Agreement containing the following statements:
    - We will support the school approach to online safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community.
    - Images taken of pupils at school events will be for personal use only and not uploaded or shared via the internet.
- As a result of supporting school policies and procedures the escalation of complaints will be through the recognised complaints procedure and not through any online social media platform.

Responsibilities of Governing Body

- To read, understand, contribute to and help promote the school's eSafeguarding policies and guidance.
- To have read and understood the applicable Acceptable Use Policy.
- To understand their professional responsibilities with regard to communication via email
- To understand their responsibilities with regard to keeping school owned information secure and not breeching the Data Protection Act.
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils as part of the wider ICT and safeguarding strategies of the school.
- To develop an overview of how the school ICT infrastructure provides safe access to the internet.
- To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.

- To support the work of the eSafeguarding Steering group and SIRO board in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafeguarding activities.
- To ensure appropriate funding and resources are available for the school to implement its eSafeguarding strategy.

**How parents and carers will be involved**

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:

- Arrange regular parent training for eSafeguarding through a parents evening
- include useful links and advice on eSafeguarding regularly in newsletters and on our school website
- Ensure that a signed copy of the children's AUP is available in each classroom for reference.
- provide each parent with a copy of ChildNet's KnowITAll for Parents information.
- include a section on eSafeguarding in the School handbook.

**Managing Digital Content**

Using images, video and sound

- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Digital images, video and sound will only be created using equipment provided by the school. . In exceptional circumstances, personal equipment may be used with permission from the headteacher provided that any media is transferred solely to a school device and deleted from any personal devices.
- Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file-name or in accompanying text online; such resources will not be published online without the permission of the staff/pupils involved.
- Written permission from parents or carers will be obtained by parents using a Policy and Consent Form for the use of Photographs, Digital Images and Video (see appendix). All staff will be made aware of any pupils whose parents have not given their consent. These children will be unable to have their images published online or in print.
- Parents and carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites (optional - unless appropriate security settings are enabled and set to maximum)
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

Storage of images

- Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment.

- The school will store images of pupils that have left the school for <XX> number of years following their departure for use in school activities and promotional resources.
- Pupils and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils.
- ***<name/names>*** has the responsibility of deleting the images when they are no longer required, or when a pupil has left the school.

**Managing ICT Systems and Access**

- Parents must sign an internet access agreement before their child/children are allowed access to the internet in school. Staff will be made aware of any children who have not been given their parents consent.
- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only the technician and County IT permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date.
- The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.
- All users will agree to an end-user Acceptable Use Policy (AUP) provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity will be monitored and checked.
- Pupils will access the Internet using the pupil log on which is configured to provide appropriate filters and restrictions to internet usage.
- Internet access will always be supervised by a member of staff.
- Members of staff will access the Internet using an individual log-on, which they will keep secure. They will ensure they log-out after each session, and not allow pupils to access the Internet through their log-on. They will abide by the school's staff AUP at all times.
- We will regularly review our Internet access in light of any issues, developments requests etc.

Wireless Networking

- Our wireless network is secure and requires both an IP and network key to enable connection. These would need to be requested from the school's technician or ICT Leader

**Filtering Internet access**

• The school uses a filtered Internet service provided by Smoothwall. This is managed in school but can be controlled by County IT.
• If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the eSafeguarding coordinator. This will then be blocked immediately by the school's technician. All incidents should be documented.
• The school will regularly review the filtering and other security systems to ensure they meet the needs of all users.

- Our school uses a proxy server to enable the creation of group policies for staff and pupils to allow different filters to be in place. This provides staff with less filtered content to websites such as YouTube which can be of educational value.
- Staff can make a request for a particular website to become unblocked to the technician.Access will be changed for STAFF ONLY.
- Requests may be made for a website to be temporarily unblocked for the use of children E.g. if they are working on a sensitive issue in PSHCE or history. Changes to the filtering of pupil access should be logged with details of the date, reason the level of filtering was changed, procedures in place to deal with any incidents arising from this change and the date the website was again blocked.

Even with filters in place, it is not possible to ever provide a 100% guarantee that pupils or staff will not come across inappropriate content at all times. The school should take all reasonable steps to minimize this risk, including education and awareness and ensuring users are aware of their role in adopting safe and responsible behaviours when using the school ICT systems.

**Passwords**

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
- pupils will have a generic 'pupil' logon to all school ICT equipment.
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school and for mobile access to the server.
- All information systems require end users to change their password at first log on.
- Users should change their passwords whenever there is any indication of possible system or password compromise
- All staff and pupils have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- All staff and pupils will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.
- All staff and pupils will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords
- Access to personal data is securely controlled in line with the school's personal data policy.
- The school maintains a log of all accesses by users and of their activities while using the system.
- Staff ipads are protected by a passcode

**Staff Training**

- Our staff receive regular information and training on eSafeguarding issues in the form of <state how, e.g. annual updates/ termly staff meetings etc>.
- As part of the induction process, all new staff receive information and guidance on the eSafeguarding policy and the school's Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of eSafeguarding and know what to do in the event of misuse of technology by any member of the school community.

- All staff will be encouraged to incorporate eSafeguarding activities and awareness within their curriculum areas

**Learning and Teaching**

- We will provide a series of specific eSafeguarding-related lessons in every year group as part of the ICT and PSCHE curriclulum. (see ESafeguarding long term plan)
- We will celebrate and promote eSafeguarding through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant eSafeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
- We will remind pupils about their responsibilities through an end-user AUP which every pupil will sign and will be displayed throughout the school.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- All pupils will be taught in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button

**Using the Internet**

- All parents will be required to sign the home-school agreement prior to their children being granted internet access within school. (see Appendix)
- Parents will be asked to read the school Acceptable Use Policy for pupil access and discuss it with their children, when and where it is deemed appropriate.
- All pupils will have the appropriate awareness training and sign the pupil Acceptable Use Policy prior to being granted internet access within school.
- All staff will have the appropriate awareness training and sign the staff Acceptable Use Policy prior to being granted internet access within school.
- Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability.
- The school will maintain a current record of all staff and pupils who have been granted access to the school's internet provision.
- Any visitor who requires internet access will be asked to read and sign the Acceptable Use Policy.
- Key Stage 1 pupils' internet access will be directly supervised by a responsible adult.
- Key Stage 2 pupils will be closely supervised and monitored during their use of the internet. Pupils will be frequently reminded of internet safety issues and safe usage.

**Using email**

- Staff and pupils should use Microsoft 365 e-mail accounts allocated to them by the school, and be aware that their use of the school e-mail system will be monitored and checked.
- In Year 2 Pupils will be allocated an individual e-mail account for their use in school
- Classes will be allocated an individual e-mail account for use by the appropriate pupils and staff. Any communication between pupils and staff should be done through the class email and NOT the staff members personal email account.
- Pupils will be reminded when using e-mail about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening e-mail from an unknown sender, or viewing/opening attachments.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately. The individual in question may have their email account suspended or permanently removed.
- Staff should not use personal email accounts during school hours or for professional purposes, especially to exchange any school-related information or documents.
- 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. A full audit trail can be made available should this become necessary.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Pupils must not reveal personal details of themselves or others in email communications. Pupils should get prior permission from an adult if they arrange to meet with anyone through an email conversation.
- Emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies are sent using a secure email address.

**Using blogs, wikis, podcasts, social networking and other ways for pupils to publish content online**

- We may use blogs to publish content online to enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. However, we will ensure that staff and pupils take part in these activities in a safe and responsible manner.
- Blogs, Wikis, Podcasts and other publishing of online content by pupils will only be used under supervision of an adult and with prior parental consent.
- Children are prohibited from using social networking sites in school, except in an educational context within a lesson where posts are monitored by staff.
- Where a class blog is being used, editing should be the overall responsibility of the staff. Any posts created by children should be done under adult supervision and approved before being published.
- If comments are used on a class blog, settings should be altered so that any comment must be approved by a member of staff before being published.
- Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside of school.

**Using video conferencing and other online video meetings**

We may use video conferencing to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear each other. However, we will ensure that staff and pupils take part in these opportunities in a safe and responsible manner.

- All video conferencing activity will be supervised by a suitable member of staff.
- Pupils will not operate video conferencing equipment, or answer calls, without permission from the supervising member of staff.
- Video conferencing equipment will be switched off and secured when not in use.
- Pupils will be given appropriate user rights when taking part in an online meeting room. They will not have host rights or the ability to create meeting rooms.
- Video conferencing should not take place off school premises without the permission of the head teacher.
- Parental permission will be sought before taking part in video conferences that involve people other than pupils and staff belonging to our school.
- Permission will be sought from all participants before a video conference is recorded.
- Video conferences should only be recorded where there is a valid educational purpose for reviewing the recording. Such recordings will not be made available outside of the school.

**Using mobile phones**

- Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent. The school mobile phone should be used instead
- Staff may need to resort to taking photos using the camera function on their mobile phone if a camera is not available. All content should be transferred and removed from the staff member's mobile phone before the end of that school day.
- If pupils bring mobile phones to school, they should be taken to the school office before the start of school to be locked in the safe until the end of the day. Pupil mobile phones are not be stored in bags/coats in the cloakrooms or classrooms.

**Using new technologies**

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- We will regularly amend the eSafeguarding policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an eSafeguarding risk.
- The acceptable use of any new or emerging technologies in use within school will be reflected within the school eSafeguarding and Acceptable Use policies.
- Prior to deploying any new technologies within school, staff and pupils will have appropriate awareness training regarding safe usage and any associated risks.

**Data Protection and Information Security**

- The school community will act and carry out its duty of care for the information assets it holds in line with its Data Protection Act 1998 commitments.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

- All computers that are used to access sensitive information should be locked (Ctrl-Atl-Del) when unattended.
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- All personal and sensitive information taken offsite will be secured through appropriate technical controls, e.g. encrypted pen stick, remote access via Foldr or use of a passcode protected ipad
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

**The school website**

The school website will not include the personal details, including individual e-mail addresses or full names, of staff or pupils.

- A generic contact e-mail address, managed by the Administrative staff, will be used for all enquiries or messages received electronically
- All content included on the school website and class blogs will be regularly monitored by the ICT coordinator, Network Manager and the head teacher.
- The content of the website will be composed in such a way that individual pupils cannot be clearly identified.
- Staff and pupils should not post school-related content on any external website without seeking permission first.

**Management of assets**

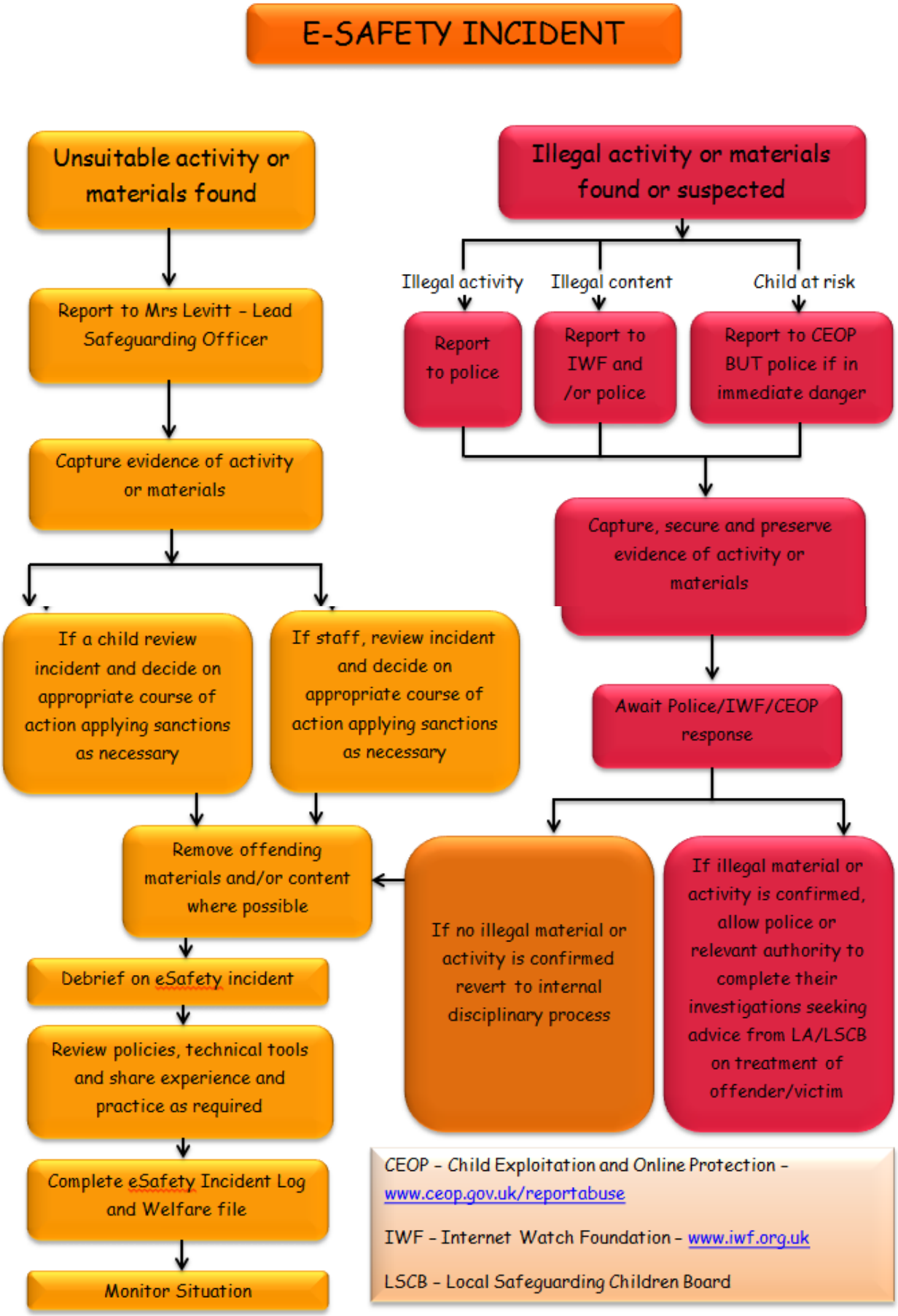
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

**Dealing with eSafeguarding incidents**

All e safety incidents will be recorded in the safety log which will include the date, details of the incident, who was involved, who it was dealt with, how it was dealt with. This log will be kept with the eSafeguarding Co-ordinator.

In most situations, where a member of staff is made aware of a possible eSafeguarding incident, they should inform the eSafeguarding coordinator, child protection coordinator / safeguarding officer or headteacher who will then respond in the most appropriate manner.

The sanctions to be used when dealing with an e safety incident can include: temporary/permanent loss of access to the internet, involvement of parents, involvement of the Head teacher, police involvement or other outside agencies. Sanctions will be in line with the schools Behaviour and Bullying Policy and with other East Riding Policies.


E-SAFETY INCIDENT
Unsuitable activity or materials found
Report to Mrs Levitt - Lead Safeguarding Officer
Capture evidence of activity or materials
If a child 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
Remove offending materials and/or content where possible
Debrief on eSafety incident
Review policies, technical tools and share experience and practice as required
Complete eSafety Incident Log and Welfare file
Monitor Situation
Illegal activity or materials found or suspected
Illegal activity
Illegal content
Child at risk
Report to police
Report to IWF and /or police
Report to CEOP BUT police if in immediate danger
Capture, secure and preserve evidence of activity or materials
Await Police/IWF/CEOP response
If no illegal material or activity is confirmed revert to internal disciplinary process
If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations seeking advice from LA/LSCB on treatment of offender/victim
CEOP - Child Exploitation and Online Protection - www.ceop.gov.uk/reportabuse
IWF - Internet Watch Foundation - www.iwf.org.uk
LSCB - Local Safeguarding Children Board