English Martyrs' Catholic School

English Martyrs, as a community centred in Christ,
strives to develop the talents of each person.
May they all be one.'

Approved/reviewed by Governors:	
September 2021	
Date of next review	**September 2022**

English Martyrs' Catholic School
eSafety and Data Security

ICT Acceptable Use

CONTENTS

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 student, 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 student and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail 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 English Martyrs' School**,** we understand the responsibility to educate our students on eSafety 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.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities.   Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and students) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Monitoring

All internet activity is logged by the school’s internet provider. These logs may be monitored by authorised staff.

Breaches

A breach or suspected breach of policy by a School employee, contractor or student may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

The ICO's new powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school’s SIRO or eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Senior Information Risk Owner. See Page 10.

Please refer to the relevant section on Incident Reporting, eSafety Incident Log & Infringements.

Acceptable Use Agreement: Students

Secondary Student Acceptable Use - Agreement / eSafety Rules

- I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network/ Learning Platform with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school e-mail address.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of students and/ or staff will only be taken, stored and used for school purposes inline with school policy and not be distributed outside the school network without the permission of the Principal.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring into disrepute.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

Dear Parent/ Carer

ICT including the internet, learning platforms, e-mail and mobile technologies have become an important part of learning in our school.   We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of eSafety and know how to stay safe when using any ICT.

Students are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their Form Tutor.

Please return the bottom section of this form to school for filing.

- - ✂ -

Student and Parent/ carer signature
We have discussed this document and ………………………………………........(student name) agrees to follow the eSafety rules and to support the safe and responsible use of ICT at English Martyrs' Catholic School.

Parent/ Carer Signature ……..…………………..…………………………….

Student Signature……………………………………………………………….

Form ………………………………… Date ………………………………

Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school eSafety coordinator or the Senior Information Risk Owner.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to students.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Principal.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout English Martyrs' Catholic School.

Signature …….…………………….………… Date ……………………

Full Name ………………………………...(printed)

Job title . . . .

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. floppy disk, CD) must be checked for any viruses using school provided anti-virus software before using them

- Never interfere with any anti-virus software installed on school ICT equipment that you use

- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know

Data Security

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

The school follows Becta guidelines Becta Schools - Leadership and management - Security - Data handling security guidance for schools (published Spring 2009)

Security

- The School gives relevant staff access to its Management Information System, with a unique ID and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- The Principal has identified a Senior Information Risk Owner (SIRO) and Asset Information Owner (AIO).
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared devices (multi-function print, fax, scan and copiers) are used

Anyone expecting a confidential/sensitive fax, should have warned the sender to notify before it is sent.

Impact Levels and Protective Marking

- Appropriate labelling of data should help schools secure data and so reduce the risk of security incidents
- Apply labelling in accordance with guidance from your Senior Information Risk Owner (SIRO)
- Most learner or staff personal data will be classed as Protect confidential

Senior Information Risk Owner (SIRO) - Business Manager

The SIRO is a senior member of staff who is familiar with information risks and the school's response. Typically, the SIRO should be a member of the senior leadership team and have the following responsibilities:

- they own the information risk policy and risk assessment
- they appoint the Information Asset Owner(s) (IAOs)
- they act as an advocate for information risk management

Information Asset Owner (IAO) – Office Manager

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. Please refer to the appendix at the back of this document showing examples of information assets a school may hold. Schools should identify an Information Asset Owner. For example, the school's Management Information System (MIS) should be identified as an asset and should have an Information Asset Owner. In this example the MIS Administrator or Manger could be the IAO.

The role of an IAO is to understand:

- what information is held, and for what purposes
- what information needs to be protected (e.g. any data that can be linked to an individual, student or staff etc including UPN, teacher DCSF number etc)
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed off

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements. In a Secondary School, there may be several IAOs, whose roles may currently be those of e-safety coordinator, ICT manager or Management Information Systems administrator or manager.

Although these roles have been explicitly identified, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed off through an authorised agency. This should 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 over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen

- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

e-Mail

The use of e-mail within most schools is an essential means of communication for both staff and students. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an e-mail in relation to their age and good network etiquette ('netiquette').

OpenHive/Capita keep emails for 7 days.

Managing e-Mail

- The school gives all staff their own e-mail account to use for all school business as a **work based tool.** This is to minimise the risk of receiving unsolicited or malicious e-mails 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; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business

- Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses

- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school (see appendix). The responsibility for adding this disclaimer lies with the account holder

- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper. Formal standard English should be used

- Students may only use school approved accounts on the school system

- All emails to students should be directly work related and comply with instructions written in the "Safer Working Practise in Educational Settings 2009".

- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows

  – Delete all e-mails of short-term value

  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

- All student e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments

- Students must immediately tell a teacher/ adult if they receive an offensive e-mail

- Staff must inform their line manager if they receive an offensive e-mail

- Contact with parents will not take place routinely by email.

- All emails to parents must be pre-authorised by the SLT Line Manager for the Department/Faculty/Year Head

- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Sending e-Mails

If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section

- e-mailing Personal, Sensitive, Confidential or Classified Information

- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate

- Do not send or forward attachments unnecessarily.

- An outgoing e-mail greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming e-mail

- School e-mail is not to be used for personal advertising

Receiving e-Mails

- Check your e-mail regularly

- Activate your ‘out-of-office’ notification when away for extended periods

- Never open attachments from an untrusted source. Consult your network manager first.

- The automatic forwarding and deletion of e-mails is not allowed

---

e-mailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted
- Where your conclusion is that e-mail must be used to transmit such data:
  - Obtain express consent from your manager to provide the information by e-mail
  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
    - Verify the details, including accurate e-mail address, of any intended recipient of the information
    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary
  - Do not send the information to any body/person whose details you have been unable to separately verify (usually by phone)
  - Send the information as an encrypted document **attached** to an e-mail
  - Provide the encryption key or password by a **separate** contact with the recipient(s)
  - Do not identify such information in the subject line of any e-mail
  - Request confirmation of safe receipt

Equal Opportunities

Students with Additional Needs

The school endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the schools' eSafety rules.

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

Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these students and young people.

eSafety

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Principal and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is the Head of ICT. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as the LA, CEOP (Child Exploitation and Online Protection).

Senior Management and Governors are updated by the Principal/ eSafety co-ordinator 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 agreements for staff, governors, visitors and students, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: student protection, health and safety and behaviour/student discipline (including the anti-bullying) policy and RE

eSafety in the Curriculum

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

- The school has a framework for teaching internet skills in ICT lessons

- The school provides opportunities within a range of curriculum areas to teach about eSafety

- Students are made 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

- Students are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities

- Students are taught about the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ staff member, or an organisation such as Studentline or CEOP report abuse button

- Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

eSafety Skills Development for Staff

- New staff receive information on the school’s acceptable use policy as part of their induction

- All staff have been made aware of individual responsibilities relating to the safeguarding of students within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart)

- Staff are reminded of expectations in an annual training session.

Managing the School eSafety Messages

- The eSafety policy will be introduced to the students at the start of each school year

- eSafety posters will be displayed

Incident Reporting, eSafety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment should be reported to the SIRO. Any unauthorised use or suspected misuse of ICT must be immediately reported to the school's eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your designated e-Safety officer or teacher for child protection. See Page 10.

eSafety Incident Log

Some incidents may need to be recorded in other places, such as the Racist Incident Log or Bullying Log.

'School name' **eSafety Incident Log**

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Principal and Governors.

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

Misuse and Infringements

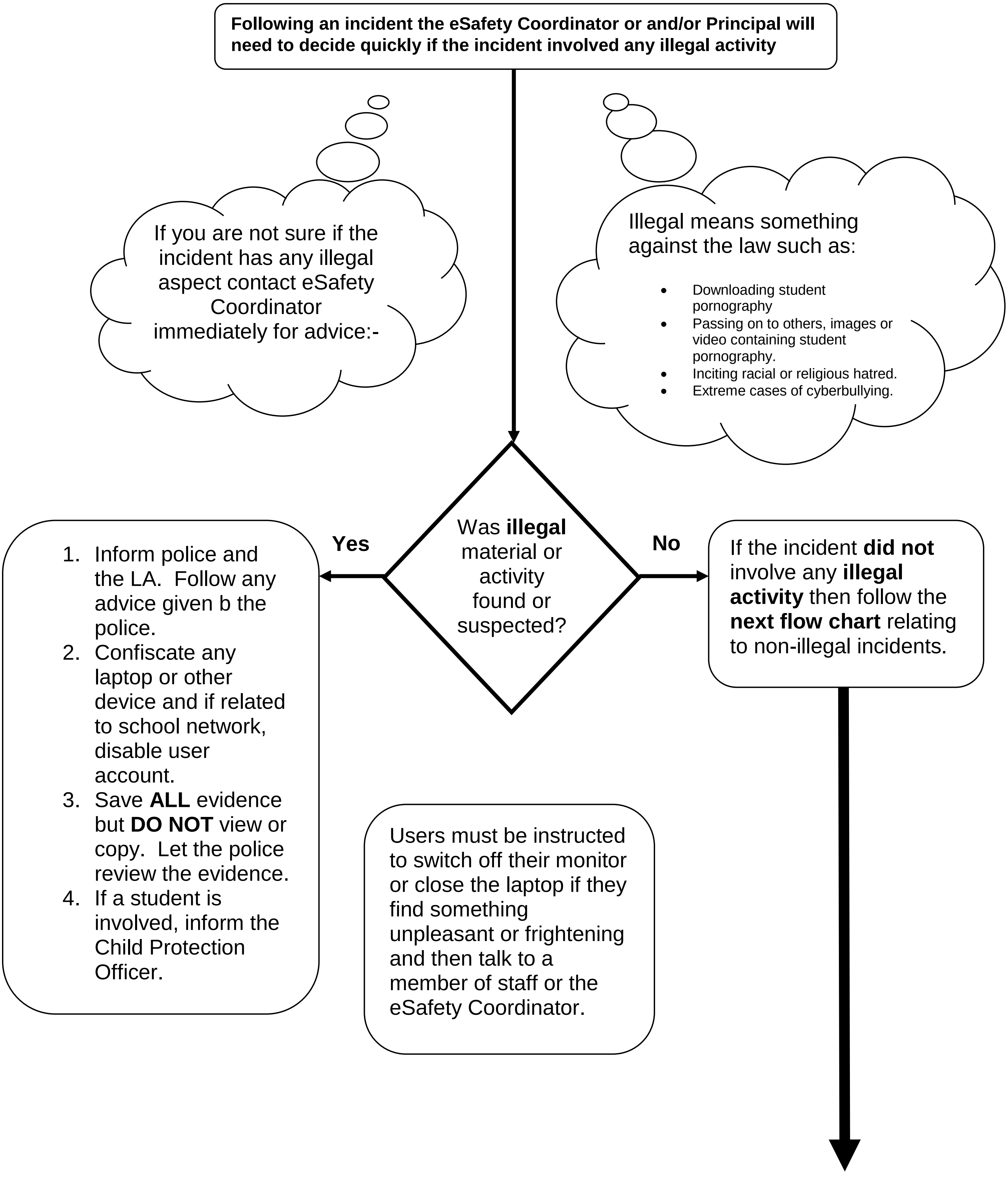
Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Principal and will be dealt with according to the school complaints procedure.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator and depending on the seriousness of the offence; investigation by senior staff and appropriate disciplinary action. This may lead to the involvement of police for very serious offences.

Flowcharts for Managing an eSafety Incident



Following an incident the eSafety Coordinator or and/or Principal will need to decide quickly if the incident involved any illegal activity

If you are not sure if the incident has any illegal aspect contact eSafety Coordinator immediately for advice:-

Illegal means something against the law such as:

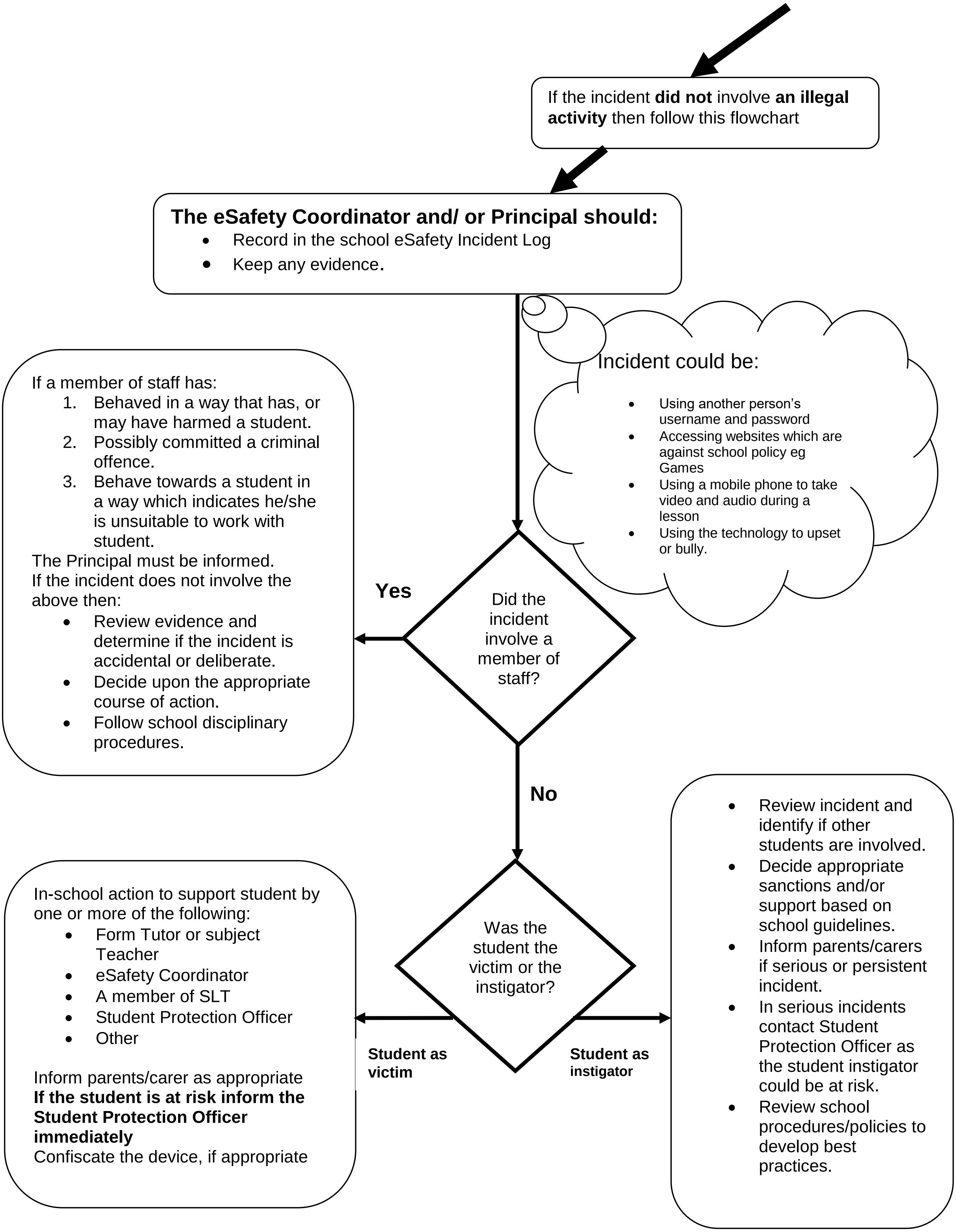
- Downloading student pornography
- Passing on to others, images or video containing student pornography.
- Inciting racial or religious hatred.
- Extreme cases of cyberbullying.

Was **illegal** material or activity found or suspected?

1. Inform police and the LA. Follow any advice given b the police.
2. Confiscate any laptop or other device and if related to school network, disable user account.
3. Save **ALL** evidence but **DO NOT** view or copy. Let the police review the evidence.
4. If a student is involved, inform the Child Protection Officer.

If the incident **did not** involve any **illegal activity** then follow the **next flow chart** relating to non-illegal incidents.

Users must be instructed to switch off their monitor or close the laptop if they find something unpleasant or frightening and then talk to a member of staff or the eSafety Coordinator.



If the incident **did not** involve **an illegal activity** then follow this flowchart

The eSafety Coordinator and/ or Principal should:

- Record in the school eSafety Incident Log
- Keep any evidence.

Incident could be:

- Using another person's username and password
- Accessing websites which are against school policy eg Games
- Using a mobile phone to take video and audio during a lesson
- Using the technology to upset or bully.

Did the incident involve a member of staff?

Yes

If a member of staff has:

1. Behaved in a way that has, or may have harmed a student.
2. Possibly committed a criminal offence.
3. Behave towards a student in a way which indicates he/she is unsuitable to work with student.

The Principal must be informed.
If the incident does not involve the above then:

- Review evidence and determine if the incident is accidental or deliberate.
- Decide upon the appropriate course of action.
- Follow school disciplinary procedures.

No

Was the student the victim or the instigator?

Student as victim

In-school action to support student by one or more of the following:

- Form Tutor or subject Teacher
- eSafety Coordinator
- A member of SLT
- Student Protection Officer
- Other

Inform parents/carer as appropriate
If the student is at risk inform the Student Protection Officer immediately
Confiscate the device, if appropriate

Student as instigator

- Review incident and identify if other students are involved.
- Decide appropriate sanctions and/or support based on school guidelines.
- Inform parents/carers if serious or persistent incident.
- In serious incidents contact Student Protection Officer as the student instigator could be at risk.
- Review school procedures/policies to develop best practices.

Internet Access

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. All use of the internet is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with students
- 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

Internet Use

- Staff should not reveal names of colleagues, customers or clients or any other confidential information acquired through the job on any social networking site or blog

It is at the Principal's discretion on what internet activities are permissible for staff and students in line with the school's character and educational mission.

Infrastructure

- Leicester City Local Authority has a monitoring solution via the East Midlands Broadband Consortium where web-based activity is monitored and recorded

- The school uses management control tools for controlling and monitoring workstations

- The school ensures that Anti-virus protection is installed and kept up-to-date.

- If there are any issues related to viruses or anti-virus software, the network manager should be informed

Managing Other Web 2 Technologies

Web 2, 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 students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking sites to students within school

- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are

- Students are taught 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

- Students 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)

- Our students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals

- Students are encouraged to be wary about publishing specific and detailed private thoughts online

- Our students are asked to report any incidents of bullying

- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with students using the VLE or other systems approved by the Principal

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers and students are actively encouraged to contribute to adjustments or reviews of the school eSafety policy through the Parent's Consultation Forum

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their student on admission to school

- Parents/ carers are required to make a decision as to whether they consent to images of their student being taken/ used in the public domain (e.g., on school website)

- Parents/ carers are expected to sign a Home School agreement containing the following statement or similar

  → **We will support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community**

- The school disseminates information to parents relating to eSafety where appropriate eg:-

  - Information and celebration evenings
  - Posters
  - Website/ Learning Platform postings
  - Newsletter items

Passwords and Password Security

Passwords

- Always use your own personal passwords to access computer based services
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Everyone is advised not to record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Staff passwords must be changed on a half term basis
- User ID and passwords for staff and students who have left the School are disabled/removed from the system within one month
- If you think your password may have been compromised or someone else has become aware of your password you must report this to the Network Manager

Password Security

Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and students 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 and Data Security
- Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username. From ***Year 7*** they are also expected to use a personal password and keep it private
- Students are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, 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 logged off.

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any School information accessed from your own PC or removable media equipment is kept secure

- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others

- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person

- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment

- Only download personal data from systems if expressly authorised to do so by your manager

- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience

- As far as possible, keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information

- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- The use of removable media is not permitted

Policy on taking, making, use and storage of Photographic Images

Purpose

The purpose of this policy is to ensure the wellbeing and protection of all members of the school community.

Rationale

This policy covers all aspects of the making, use, storage and retrieval of photographic images of members of the school. This includes all conventional photographs, all forms of digital photography, still and moving images.

1. Photography for the purposes of school identification and security

The school may request photographs of governors, employees, volunteer helpers and students for purposes of identification. These images may be held in paper files or electronically. Photographs of all students will be held on the school database.

CCTV cameras monitor movement throughout the site both externally and internally. Images are recorded digitally and held for security purposes for seven days.

2. Photography for educational purposes

Photographs of students' work may be taken for the purpose of Assessment and Recording (e.g. videoing of class work/assessments).

Photographs may be taken of school events e.g. sports fixtures, assemblies, liturgies, concerts, theatrical productions, school visits, retreats etc., in order to celebrate students' work.

Students studying courses in photography are expected to observe this policy and the spirit of the policy, as advised by their photography/art teacher.

3. Photographs for school communication

Photographs may be taken for school brochures, newsletters, prospectus and the media.

4. Portrait photography

Photographs may be taken of class groups and year groups as a memento for those in the particular groups.

Individual portrait photographs of a student may be taken by a professional 'school photographer' at the request of the student's parents.

All photographs taken for the purposes outlined above will be taken by a designated member of the school or employee/contractor as approved by the Principal.

5. Display

Photographs for purposes of security and identification will not be displayed.

Photographs of the life of the school will be displayed throughout the school. The names of individual students will not be displayed alongside their photographs.

Photographs of the life of the school may be displayed in newsletters, website, prospectus and the media. The names of individual students will not be displayed alongside their photographs, but may sometimes be used in the body of the text, except for student year books.

Some photographic images will be displayed on the school website.

6. Consent

Parents will be informed in writing of this policy and asked to acknowledge receipt.

Any parent who does not wish their child to be photographed for the purpose outlined in categories 3, 4 and 5 will be asked to inform the Principal in writing.

When photographs are taken for the purposes outlined in categories 3, 4 and 5 above a student whose parents do not wish him/her to participate should remind the supervising member of staff.

The school will treat as a disciplinary matter the misuse of photographic imaging of any member of the community.

Permission to use the school photographic images on websites must always be obtained prior to their display.

7. Child Protection

For the purposes of Child Protection photographic images may not be made at school events by anyone without the permission of the Principal. 'Official' photographs/ recordings will be made available to parents on request. Photographic images may not be taken using mobile telephones.

8. Looked After Children

Photographs of students who are in the care of the Local Authority will only be taken once the appropriate permissions have been received by the Designated Child Protection Officer.

9. Copyright

The governing body asserts and retains copyright of all images made with school equipment or on behalf of the school. Copyright images may only be used with prior permission.

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you

- The school logs ICT equipment issued to staff and record serial numbers as part of the school's inventory

- The school does not allow visitors to plug their ICT hardware into the school network points (unless special provision has been made).

- Ensure that all ICT equipment that you use is kept physically secure

- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990

- It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive

- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted

- Privately owned ICT equipment should not be used on a school network without prior permission from the principal.

- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled

- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person

- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:

  - maintaining control of the allocation and transfer within their Unit
  - recovering and returning equipment when no longer needed

- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

This section covers such items as laptops, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on School systems and hardware will be monitored in accordance with the general policy

- Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey

- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis

- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades

- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support

- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight

- Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for students and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to students 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.

Personal Mobile Devices (including phones)

- 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 student or parent/ carer using their personal device

- Students are not allowed to bring personal mobile devices/phones to school.

- Facilities are available for safe storage where a mobile device is required after school.

- The school is not responsible for the loss, damage or theft of any personal device

- Permission must be sought before any image or sound recordings are made of members of the school community

- Students bringing devices into school must ensure there is no inappropriate or illegal content on the device

- Visitors – Parents attending school events must not use mobile devices to record the event.

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages using school devices 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 phones, laptops and PDAs for offsite visits and trips, only these devices should be used

- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

Servers

- Limit access rights ~ only Network Managers and Head of ICT have full rights.
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification
- Data must be backed up regularly
- Back up discs must be securely stored in a fireproof container
- Back up media stored off-site must be secure

Smile and Stay Safe Poster

eSafety guidelines to be displayed throughout the school

MILE **stay safe**

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a ‘friend’

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Systems and Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC

- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you

- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information

- Ensure you log off before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access

- Do not introduce or propagate viruses

- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or LCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)

- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act

- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998

- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

Telephone Services

- You may make or receive personal telephone calls provided:

  1. They are infrequent, kept as brief as possible and do not cause annoyance to others

  2. They are not for profit or to premium rate services or international calls

- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused

- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases

- Ensure that your incoming telephone calls can be handled at all times

- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office. If you do not have a copy, please ask your unit manager

Mobile Phones

- Report the loss or theft of any school mobile phone equipment immediately

- School SIM cards must only be used in school provided mobile phones

- You must not send text messages to premium rate services

Writing and Reviewing this Policy

Staff and Student Involvement in Policy Creation

- Staff and students have been involved in making/ reviewing the Policy for ICT Acceptable Use through eSafety and Data Security

Review Procedure

Staff should discuss with the eSafety coordinator any issue of eSafety that concerns them

Staff should discuss with the SIRO/AIO any issue of data security that concerns them

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

The policy will be amended if new technologies are adopted or Central Government change the law, orders or guidance in any way

This policy has been adopted by the Governing Body on……………………………….

Remote Access

- School staff who need to have remote access to servers need to be pre-authorised by both the SIRO and eSafety Officer and a log kept (Request for Access 1 Pro-Forma)

- Only use equipment with an appropriate level of security for remote access

- Staff are responsible for all activity via your remote access facility

- To prevent unauthorised access to School systems, keep all access information, logon IDs and PINs confidential and do not disclose them to anyone

- Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment

Request to be allowed to use **remote access** to the **servers** from **off** the English Martyrs school site (Request for Access 1)

Date requested	Date and time access to be used	Reason for access?	Reason why it cannot be carried out at school?	Person requesting access	SIRO & E-safety officer confirmation of access. (both required to grant access)