



RALPH SADLEIR SCHOOL



ICT Acceptable Use Policy Incorporating eSafety and Data Security

Department:	ICT
Date of issue:	August 2012
Review date:	June 2017
Next review date:	June 2019

CONTENTS

Introduction.....	1
Monitoring.....	3
Breaches	4
Incident Reporting.....	4
Acceptable Use Agreement: Pupils.....	5
Acceptable Use Agreement: Staff, Governors and Visitors.....	Error! Bookmark not defined.
Staff Professional Responsibilities	8
Computer Viruses.....	9
Data Security	10
Security	10
Disposal of Redundant ICT Equipment Policy.....	11
E-mail	12
Managing e-Mail	12
Sending e-Mails.....	13
Receiving e-Mails	13
E-mailing Personal, Sensitive, Confidential or Classified Information.....	14
Equal Opportunities	15
Pupils with Additional Needs.....	15
eSafety	16
eSafety - Roles and Responsibilities.....	16
eSafety in the Curriculum.....	16
eSafety Skills Development for Staff.....	17
Managing the School eSafety Messages	17
Incident Reporting, eSafety Incident Log & Infringements.....	18
Incident Reporting.....	18
eSafety Incident Log.....	18
Misuse and Infringements.....	19
Flowcharts for Managing an eSafety Incident	20
Internet Access.....	21
Managing the Internet.....	21
Internet Use	21
Infrastructure.....	21
Managing Other Online Technologies.....	22

Parental Involvement	23
Passwords and Password Security	24
Passwords	24
Password Security	25
Zombie Accounts	25
Personal or Sensitive Information	26
Protecting Personal, Sensitive, Confidential and Classified Information	26
Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media	26
Remote Access	27
Safe Use of Images	28
Taking of Images and Film	28
Consent of Adults Who Work at the School	28
Publishing Pupil's Images and Work	28
Storage of Images	29
School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media	30
School ICT Equipment	30
Portable & Mobile ICT Equipment	31
Mobile Technologies	32
Removable Media	33
Servers	33
Smile and Stay Safe Poster	34
Systems and Access	35
Telephone Services	36
Mobile Phones	36
Writing and Reviewing this Policy	38
Staff and Pupil Involvement in Policy Creation	38
Review Procedure	38
Current Legislation	39
Acts Relating to Monitoring of Staff eMail	39
Other Acts Relating to eSafety	39
Acts Relating to the Protection of Personal Data	411

Introduction

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

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

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook, Twitter, Snap Chat and Instagram
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

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 and that some have minimum age requirements, usually 13 years.

At **Ralph Sadleir**, we understand the responsibility to educate our pupils 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 pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, External Storage devices, Smart phones, tablets, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, smart phones, camera phones, portable media players and more).

Monitoring

The ICT Manager / ICT Subject Leader / Head, may inspect any ICT equipment owned or leased by the school at any time without prior notice. ICT authorised staff may monitor, intercept, access, inspect, record and disclose e-mails, internet/intranet use and any other electronic communications (data, voice or image) involving its pupils or school staff without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

The ICT Manager / ICT Subject Leader / Head, without prior notice, may access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account

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

Breaches

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

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's office new powers to issue monetary penalties came into force on 6 April 2010, allowing the ICO 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

For pupils, policy breaches may also lead to criminal or civil proceedings.

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 ICT department or Head. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the ICT Manager.

Acceptable Use Agreement: Pupils

- I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, social media, etc. for school purposes.
- I will not download or install software on school technologies. I will only log on to the school network 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 for school related purposes.
- I will make sure that all ICT communications with pupils, 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. Images of pupils and/ or staff will only be taken, stored and used for school purposes in line with school policy. These are not to be distributed outside the school network without the permission of the pupil, their parents or a member of staff.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring them 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 parents / carer may be contacted.

Dear Parent/ Carer

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

Pupils 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 class teacher or school eSafety coordinator.

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

✂

Pupil and Parent/ carer signature

We have discussed this document and(pupil name) agrees to follow the eSafety rules and to support the safe and responsible use of ICT at Ralph Sadleir School.

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.

Parent/ Carer Signature

Pupil Signature.....

Form Date

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 adhere to this policy at all times to its contents. Any concerns or clarification should be discussed with ICT Support Team or SLT.

- I will only use the school's email / Internet / Social Media Services, 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 pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, Facebook, Twitter, Snap Chat, Instagram or other social media details to pupils.
- 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 Head. Personal or sensitive data taken off site must be encrypted.
- If leaving the employment of Ralph Sadleir school any ICT equipment belonging to the school must be returned and any school related data; especially that of a sensitive nature, must be returned the school or deleted from personal devices and equipment, by a member of the ICT department where possible.
- I will not install any hardware or software without prior consultation with the ICT Support Team
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and /or staff will only be taken, stored and used for professional purposes in line 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 Headteacher.
- 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 Headteacher.
- 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 and understand that any breach of this could lead to disciplinary action.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

All staff are to following this code of conduct and to support the safe and secure use of ICT throughout the school. Failure to do so may result in disciplinary procedures being taken.

Staff Professional Responsibilities



PROFESSIONAL RESPONSIBILITIES **When using any form of ICT, including the Internet,** **in school and outside school**



For your own protection we advise that you:

- › Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.



- › Do not talk about your professional role in any capacity when using social media such as Facebook and YouTube.

- › Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.



- › Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.



- › Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.

- › Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.



- › Only take images of pupils and/ or staff for professional purposes, in accordance with school policy and with the knowledge of SLT.

- › Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- › Ensure that your online activity, both in school and outside school, will not bring your organisation or professional role into disrepute.



You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation.

The HSCB eSafety subgroup have produced a clear summary of **professional responsibilities related to the use of ICT** which has been endorsed by unions. To download visit <http://www.thegrid.org.uk/eservices/safety/policies.shtml>

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. Ext Hard Drives, USB Mem stick, 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 ICT team
- If you suspect there may be a virus, spyware, malware, ransomware or any other such infection on any school ICT equipment, stop using the equipment, ensure the machine is turned off immediately and disconnected from the network, then contact the ICT department immediately. The ICT department will advise you what actions to take and be responsible for advising others that need to know

Data Security

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

The Local Authority guidance documents listed below

[HGfL: School Admin: School Office: Data Protection and Freedom of Information](#)

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
- Staff have read the relevant guidance documents available on the SITSS website concerning 'Safe Handling of Data' available on the grid at <http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata>)
- 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 copiers (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.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency or via the Hertfordshire Business Services (HBS) disposal scheme. 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
- Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

<http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx>

http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=e

Data Protection Act 1998

http://www.ico.gov.uk/what_we_cover/data_protection.aspx

Electricity at Work Regulations 1989

http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

- The school will maintain a comprehensive inventory of all its ICT equipment.
- A disposal record will include:
 - Date item disposed of
 - Authorisation for disposal, including:
 - verification of software licensing
 - any personal data likely to be held on the storage media? *
 - How it was disposed of eg waste, gift, sale
 - Name of person & / or organisation who received the disposed item

* if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

- 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 pupils. 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 pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving e-mails.

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 pupils, 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. 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
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- 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 pupil 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
 - Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail
 - Staff must inform the ICT department or the SLT if they receive an offensive e-mail
-

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
 - Use your own school e-mail account so that you are clearly identified as the originator of a message
 - 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. Whenever possible, send the location path to the shared drive rather than sending attachments
 - 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
- Never open attachments from an un-trusted source; Consult the ICT Manager first.
- Even if an email address is from a known sender, consult IT first if it does not seem correct at first due to Email address spoofing.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of e-mails is not allowed

E-mailing Personal, Sensitive, Confidential or Classified Information

- 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 anyone/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

In exceptional circumstances, the County Council makes provision for secure data transfers to specific external agencies. Such arrangements are currently in place with:

- Hertfordshire Constabulary
- Hertfordshire Partnership Trust

Equal Opportunities

Pupils with Additional Needs

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

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

Where a pupil 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 children and young people.

eSafety

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this has been designated this role as a member of the senior leadership team. 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 Herts LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and governors are updated by the Head/ 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 pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home-school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE

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 pupils 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/ PSHE lessons
- The school provides opportunities within a range of curriculum areas to teach about eSafety
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities

- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

eSafety Skills Development for Staff

- Our staff receive regular information and training on eSafety issues in the form of website updates from organisations such as CEOP, and standard learning methods as courses, videos, newsletters
- 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 children 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)
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

Managing the School eSafety Messages

- We Endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used
- The eSafety policy will be introduced to the pupils at the start of each school year
- eSafety posters will be prominently displayed

Incident Reporting, eSafety Incident Log & Infringements

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 eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your ICT Manager.

eSafety Incident Log

Some incidents may need to be recorded in other places, such as Sims.net, if they relate to a bullying or racist incident.

'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 Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying should be recorded on the 'Integrated Bullying and racist Incident Record Form 2'

Date & time	Name of pupil or staff member	Male or Female	Room and 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 Head teacher. Incidents should be logged and the **Hertfordshire Flowcharts for Managing an eSafety Incident** should be followed.

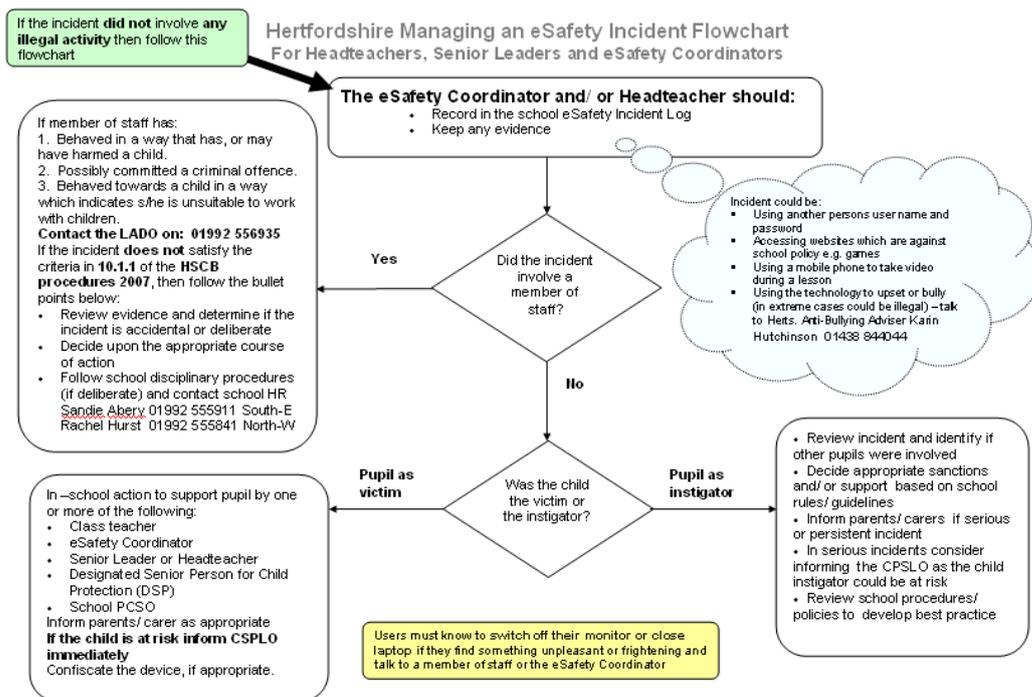
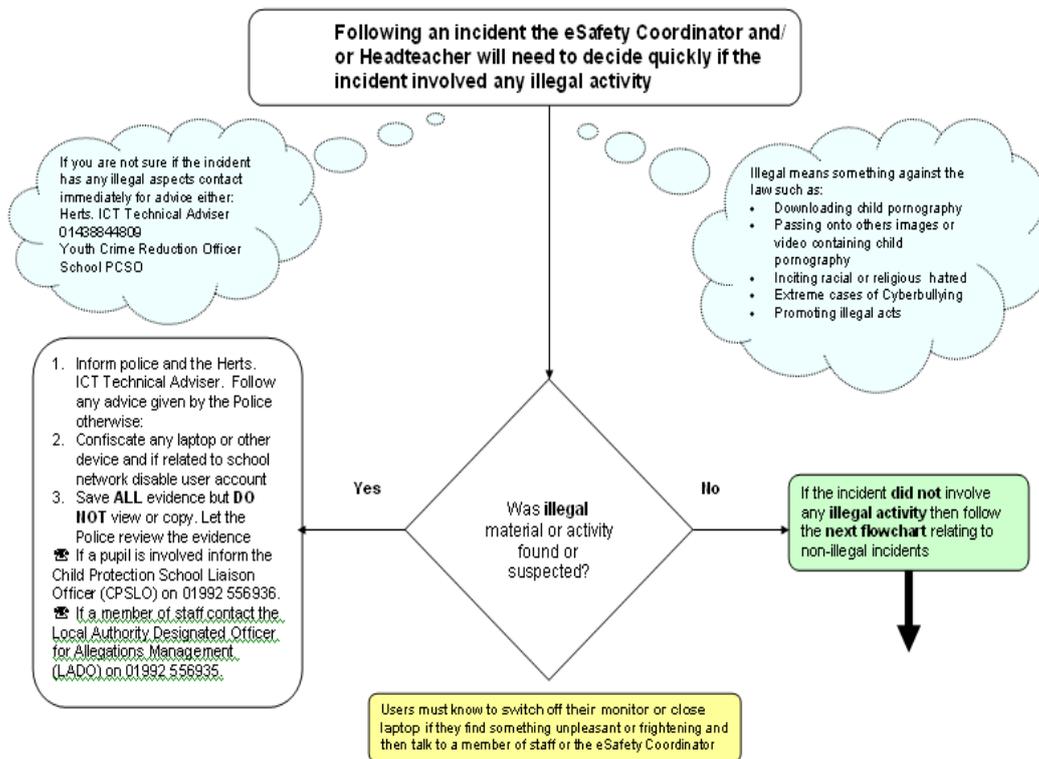
Inappropriate Material

- 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, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)
- Users are made aware of sanctions relating to the misuse or misconduct.

Flowcharts for Managing an eSafety Incident

<http://www.thegrid.org.uk/eservices/safety/research/incident.shtml>

Hertfordshire Flowchart to support decisions related to an Illegal eSafety Incident
For Headteachers, Senior Leaders and eSafety Coordinators



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 black hole of misinformation and a potential risk to young and vulnerable people. All use of the **Hertfordshire Grid for Learning (HGfL)** is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- The school maintains students who will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology
 - Staff will preview any recommended sites before use
 - Raw image searches are discouraged when working with pupils
 - If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
 - All users must use websites safe search features.
 - 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

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience
- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog
- On-line gambling or gaming is not allowed

It is at the Headteacher's discretion on what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- Hertfordshire Local Authority has a monitoring solution via the Hertfordshire Grid for Learning where web-based activity is monitored and recorded

- School internet access is controlled through the LA's web filtering service. For further information relating to filtering please go to <http://www.thegrid.org.uk/eservices/safety/filtered.shtml>
- Ralph Sadleir is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- The school uses management control tools for controlling and monitoring workstations
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate
- It is the responsibility of the school, by delegation to the ICT Department, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is neither the school's responsibility nor the ICT Managers to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the ICT Department for a safety check first
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Headteacher/ICT Department
- If there are any issues related to viruses or anti-virus software, the ICT Department should be informed

Managing Other Online Technologies

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

- At present, the school endeavors to deny access to social networking sites to

pupils within school

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Pupils 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
- Pupils 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 pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online
- Our pupils are asked to report any incidents of bullying to the school
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using systems approved by the Headteacher
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored <http://www.coppa.org/comply.htm>

For more information follow this link

http://www.thegrid.org.uk/eservices/safety/social_networking/index.shtml

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.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school
- Parents/ carers are required to make a decision as to whether they consent to images of their child 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 in the form of;

- Information and celebration evenings
- Posters
- Website
- Newsletter items

http://www.thegrid.org.uk/eservices/safety/documents/mind_the_gapv2.pdf

Passwords and Password Security

Passwords

Please refer to the document on the grid for guidance on How to Encrypt Files which contains guidance on creating strong passwords and password security

<http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata>

- **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 to an entirely different password, not a variant on the existing one
- Do not 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
- Passwords must contain a minimum of six characters and be difficult to guess
- Passwords are not to be written down and left unattended
- User ID and passwords for staff and pupils who have left the School are removed from the system within *1 week of departure*

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team

Password Security

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

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security
- Users are provided with an individual network, email and Management Information System (where appropriate) log-in username. From Year 7 pupils are also expected to use a personal password and keep it private
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, email and /or MIS system including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school network is *1 minute*.
- In our school, all ICT password policies are the responsibility of the ICT Manager and all staff and pupils are expected to comply with the policies at all times

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left
- Prompt action on disabling accounts will prevent unauthorized access
- Regularly change generic passwords to avoid unauthorized access (Microsoft® advise every 42 days)

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 you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access. Do not rely on the automatic lock process.
- 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 copiers (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
- 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

- Ensure removable media is purchased with encryption
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access. Devices that require access to VPN software are to be virus checked by IT before it being installed.
- To prevent unauthorised access to school systems, keep all VPN access information such as telephone numbers, logon IDs confidential and do not disclose them to anyone
- Select passwords to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- 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

Safe Use of Images

Taking of Images and Film

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

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment

Consent of Adults Who Work at the School

- Permission for the school to use images of all staff who work at the school is sought on induction.

Publishing Pupil's Images and Work

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

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- in teaching materials used within school for educational purposes
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

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

Parents/ 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. Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published in any documents, including anything that is published on the school website and newsletters.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Storage of Images

- Images/ films of pupils are stored on the school's network. They should not be stored on personal equipment such as mobile telephones, tablets or cloud storage.
- With the express permission of a member of SLT, staff may take images/films of pupils on personal devices such as mobile telephone/tablets. The images must be emailed to the designated person using a school email address and then stored on the school's network. All images/films of pupils on personal devices must then be deleted. This includes cloud storage.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to school staff and pupils within the confines of the school network

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
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities if available
- 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
- It is recommended that a time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a school network without express permission from the ICT Manger
- On termination of employment, resignation or transfer, return all ICT equipment to the ICT department. 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, Notebooks, Tablets 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 department, 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 children and young people. Many existing mobile technologies such as portable media players, Tablets gaming devices, mobile and smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

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 pupil or parent/carer using their personal device
- Pupils are allowed to bring personal mobile devices/phones to school but must leave them in a secure location within the admin department when they arrive at school.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- Where the school provides mobile technologies such as phones, laptops and tablets 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

Removable Media

If storing/transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section 'Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media' - Page 28

- Only use recommended removable media
- Store all removable media securely
- Removable media must be disposed of securely by the ICT department

Servers

- Always keep servers in a locked and secure environment
- Limit access rights
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification
- Back up tapes should be encrypted by appropriate software
- Data must be backed up regularly
- Back up tapes/discs must be securely stored in a fireproof container
- Back up media stored off-site must be secure
- Remote back ups should be automatically securely encrypted.

Smile and Stay Safe Poster

eSafety guidelines to be displayed throughout the school

Cyberbullying

MILE and stay safe

Staying safe and not being a victim of cyberbullying means keeping your personal details private, such as full name and phone number. Never let anyone know your password and try to choose hard to guess passwords that include numbers and symbols such as \$.

Make sure you think before sending a text or image of yourself or someone else. Remember that once some information about you or others has been sent by text or posted on a social network, such as Facebook - it can be made public and may stay online for ever!

If you send messages to others remember to think about the impact of your words and images. If you receive a rude, nasty or unpleasant message or image about someone else do not forward as you could be helping the bully, or be accused of being the bully or even break the law.

Let a parent, carer, teacher, anti-bullying coordinator or trusted adult know if you are ever bullied. You can also call Childline on **0800 1111** in confidence.

Emails, text messages, chat rooms and social networks are some of the technologies that are used to cyberbully. These technologies will all contain evidence of any bullying and this evidence can be kept and used as proof of cyberbullying.

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 equipment
- 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 lock your screen 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
- Ensure that you log off from the PC completely when you are going to be away from the computer for a longer period of time
- 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 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
 3. They conform to this and other relevant school policies.
- 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

- You are responsible for the security of your school mobile phone. Always set the PIN code on your school mobile phone and do not leave it unattended and on display (especially in vehicles)
- Report the loss or theft of any school mobile phone equipment immediately
- The school remains responsible for all call costs until the phone is reported lost or stolen
- You must read and understand the user instructions and safety points relating to the use of your school mobile phone prior to using it
- School SIM cards must only be used in school provided mobile phones
- All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default
- You must not send text messages to premium rate services

- In accordance with the Finance policy on the private use of School provided mobiles, you must reimburse the school for the cost of any personal use of your school mobile phone. This includes call charges incurred for incoming calls whilst abroad. [To assist you in identifying personal use, add * to the end of the number being contacted, these will be shown separately on your bill]. Payment arrangements should be made through your finance administrator
- Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so

Writing and Reviewing this Policy

Staff and Pupil Involvement in Policy Creation

- Staff and pupils have been involved in making/ reviewing the Policy for ICT Acceptable Use.

Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them

There will be an on-going opportunity for staff to discuss with the Headteacher/ICT Manager any issue of data security that concerns them

This policy will be reviewed at least every 3 years 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 orders or guidance in any way

This policy has been read, amended and approved by the Senior Leadership Team and Curriculum and Achievement Committee on 6th June 2017 and distributed to staff thereafter.

Current Legislation

Acts Relating to Monitoring of Staff eMail

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

<http://www.hmso.gov.uk/acts/acts1998/19980029.htm>

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

<http://www.hmso.gov.uk/si/si2000/20002699.htm>

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

<http://www.hmso.gov.uk/acts/acts2000/20000023.htm>

Human Rights Act 1998

<http://www.hmso.gov.uk/acts/acts1998/19980042.htm>

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a

position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of “*Children & Families: Safer from Sexual Crime*” document as part of their child protection packs.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual’s motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person’s password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone’s work without obtaining their author’s permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else’s material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx