MONK'S WALK SCHOOL
KNIGHTSFIELD
WELWYN GARDEN CITY
HERTFORDSHIRE
AL8 7NL
www.monkswalk.herts.sch.uk

admin@monkswalk.herts.sch.uk
01707 322846

e-Safety policy

Date of issue:	May 2019
Policy review date:	May 2021

Policy Status	Non-Statutory, SLT Approved
Responsible member of SLT:	Toby Eager-Wright

Adapted from Herts for Learning 2016
Model policy for schools: e-Safety and Data Security

Guidance policy for 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 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, e.g. Facebook, Twitter, Instagram, Snapchat etc.
- Mobile / Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets, gaming devices and smart watches
- 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 (13 years in most cases).

At Monk's Walk School, we understand the responsibility to educate our pupils on e-Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and others 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 community 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, Trustees, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Monitoring

Authorised staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any authorised staff member will be happy to comply with this request.

Authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, 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 2018, or to prevent or detect crime.

Authorised staff may, without prior notice, 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 that provider (eg Herts for Learning Ltd).

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the General Data Protection Regulation

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

A breach or suspected breach of policy by a school employee, contractor 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 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 relevant responsible person. Additionally, all security

breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are the Network Manager and team.

Please refer to the relevant section on Incident Reporting, e-Safety Incident Log & Infringements.

Acceptable Use Agreement: Pupils – Secondary

- I will only use the computer systems and services (e.g. Internet, email, apps) in school for school purposes and with the permission of school staff
- I will respect the schools equipment. Anything that is not working as expected will be reported to the teacher
- I will not download or install software onto the school computers or network
- I will only log onto the school system or other school services with my own username and password
- I will not reveal my username and password to anyone else, and I am responsible for my own school accounts
- If I think my account has become compromised, I will notify the teacher and get my passwords reset if required
- I will only use my school email address for school related purposes
- I will ensure any communication with teachers and others is responsible and polite
- I will be responsible for my Internet Browsing, this also includes the resources I access and the language I use online
- I will not browse, download, upload, forward or show material that is illegal, inappropriate or offensive. If I come across something accidently I will inform my teacher or another member of staff
- I understand that not everything I see online may be true, accurate or genuine. I understand that some people on the Internet maybe not who they say they are and I need to be very cautious about contacting anyone outside of school, as they may put me at risk.
- I will not give out my own or anyone else's personal information, which includes, but not limited to: name, phone or mobile number, address, interests, schools or clubs, pictures to anyone online.
- If I need to take pictures or video of other students or staff, I must have their consent and store these in school only, or on the school system, and not pass them on outside school using any means.
- I will ensure that my online activity inside and outside of school will not cause the school, staff, students or others distress, or bring the school community into disrepute. This includes but not limited to the sharing of images, video, sounds or messages
- I will support the school approach to online safety and not deliberately upload or add any images, sounds, video or messages that could upset a member of the school community
- I will respect the privacy of others and their work online at all times
- I will not respond to hurtful behaviour online but will report hurtful behaviour to a member of school staff
- I will not attempt to compromise the school system or go beyond what I have access to
- I will not attempt to bypass or remove the schools Internet Filtering system
- I will not attempt to disable the Antivirus system or circumvent it
- I understand that my Internet usage is monitored and logged and that any school system I use can be checked at any time by the Network Department or teachers
- I understand my school network area is monitored and can be checked at any time, and inappropriate files may be removed without warning
- I will not use my own devices to connect to the schools main network. If I am found using a device that is plugged into the main network it will be confiscated
- I will not sign up for any services that are age restricted if I am under the age
- I understand that these rules are designed to keep me safe and if they are not followed I may be sanctioned by any means the school deems appropriate, and my parent/carer may be contacted.

The acceptable use agreement for pupils is printed in the student planner and must be read and signed by students and parents

Acceptable Use Agreement: Staff, Trustees and Visitors

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 Network Manager or e-safety co-ordinator.

- I will only use the computer systems and services (e.g. Internet, email, apps) in school, for school purposes

- I will respect the schools equipment and anything that is not working as expected will be reported to the Network Department
- I will not download or try to install software onto the school computers or network (Network Department members exempt)
- I will only log onto the school system or other school services with my own username and password
- I will not reveal my username and password to anyone else, and I am responsible for my own school accounts
- If I think my account has become compromised, I will notify the Network Department and get my passwords reset if required
- I will only use my school email address for school related purposes
- I will ensure any communication with others is responsible and polite
- I will not browse, download, upload, forward or show material that is illegal, inappropriate or offensive.
- I will not give out my own or anyone else's personal information, which includes, but not limited to: name, phone or mobile number, address, interests, schools or clubs, pictures to anyone online.
- I will not divulge any of my social media accounts such as Facebook, Twitter, Instagram, Snapchat etc to current students.
- If I need to take pictures or video of students or staff, I must have their consent and store these in school only, or on the school system, and not pass them on outside school using any means.
- I will ensure that my online activity inside and outside of school will not cause the school, staff, students or others distress, or bring the school community into disrepute. This includes but not limited to the sharing of images, video, sounds or messages
- I will support the school approach to online safety and not deliberately upload or add any images, sounds, video or messages that could upset a member of the school community
- Student communication is to be by authorised means only. A list of authorised software/websites can be found in the online services register document kept in Teacher drive T:\Admin\GDPR. If any conversations develop that exceed normal student-teacher relationships, e.g. student demonstrates vulnerability, or other examples covered in the safeguarding handbook, please report on CPOMS. Do not put yourself at risk.
- I will respect the privacy of others and their work online at all times
- I will not attempt to compromise the school system or go beyond what I have access to
- I will not attempt to bypass or remove the schools Internet Filtering system
- I will not attempt to disable the Antivirus system or circumvent it
- I understand that my Internet is monitored and logged and that any school system I use can be checked at any time by the Network Department
- I understand my school network area is monitored and can be checked at any time
- I understand that my school email can be monitored and checked at any time
- I will not use my own devices (laptop, mobile etc.,) to connect to the schools main network. Any devices that do connect will be removed.
- Any software or hardware requirements for departments has to be approved by the Network Department
- I will encrypt any personal or sensitive information that is being sent externally via email to authorised parties
- I will not remove or send any personal data off the school systems about staff or students to unauthorised third parties. This includes but not limited to email, cloud storage, removable media.
- I will not store any personal information about students or staff on personal devices such as USB drives, Laptops, Computers.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

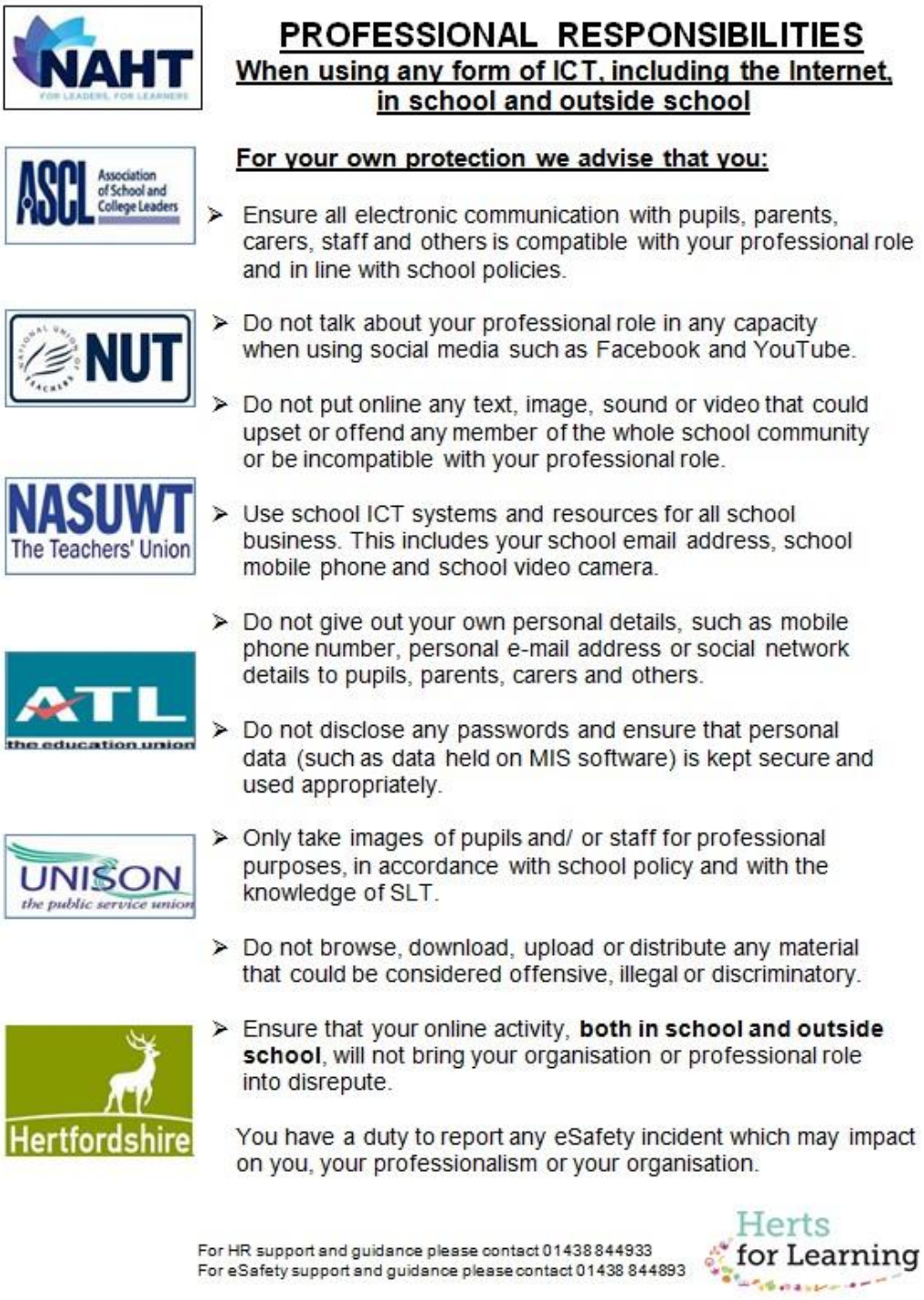
Signature: ……..……...…… Date: ……

Full Name: ……..... (printed)

Job title: ……

Staff Professional Responsibilities

The HSCB e-safety subgroup group 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



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.

For HR support and guidance please contact 01438 844933
For eSafety support and guidance please contact 01438 844893

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school ICT equipment.
- 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. HCC guidance documents can be found at:

http://www.thegrid.org.uk/info/dataprotection/index.shtml#data

Security

- The school gives relevant staff access to its Management Information System, with a unique username 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)
- Leadership have identified relevant responsible persons as defined in the guidance documents on the SITSS website (available - http://www.thegrid.org.uk/info/traded/sitss/)
- 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 mopiers (multi-function print, fax, scan and copiers) are used

Cloud Based Data

- Use of cloud based services for professional purposes must be authorised by the Network Manager. The Network Manager will certify that Data Protection and all other requirements are met by the cloud service provider.
- The use of such services must comply with all other existing IT policies.
- Staff should create professional accounts on these services using their work email address, separate from any accounts they use for personal data storage, manipulation or exchange. Personal cloud service accounts must not be used for the storage, manipulation or exchange of any sensitive or confidential information. Onedrive is to be used for school purposes only.
- Staff may not share login details for these services with others. However, staff should inform IT of their login credentials for these services to maintain continuity of service.
- The use of these services should comply with all laws and regulations governing the handling of personally identifiable information, financial data, or any other sensitive or confidential information.
- Staff should not require pupils to sign up for these services without the approval of the Network Manager and the e-Safety Co-ordinator

Access to Information
The Network Manager will maintain an Access Control List which will be used to grant access to information on a principle of least privilege on the network.

The Network
- Staff and pupils will be restricted from viewing any files outside of their granted access area.
- All files should be stored only in the appropriate area of the network to ensure that those able to access the information are authorised to do so.
- Sensitive and confidential information containing identifying personal details about pupils should only be stored on the T or W drive.
- If USB sticks are to be used, they have to be encrypted with Bitlocker. If they are not encrypted, then they will only be read only.

Relevant Responsible Persons
Senior members of staff should be familiar with information risks and the school's response. Sometimes called a SIRO, there should be a member of the senior leadership team who has the following responsibilities:
- they lead on the information risk policy and risk assessment
- they advise school staff on appropriate use of school technology
- they act as an advocate for information risk management

The Office of Public Sector Information has produced *Managing Information Risk*, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support relevant responsible staff members in their role.

Information Asset Owner (IAO)
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. A responsible member of staff should be able to identify across the school:
- what information is held, and for what purposes
- what information needs to be protected, how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed of

As a result, this manager 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 individuals, whose roles involve such responsibility.

However, it should be clear to all staff that 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 of 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
- Disposal of any ICT equipment will conform to:
  The Waste Electrical and Electronic Equipment Regulations 2013
  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 2018
  https://ico.org.uk/for-organisations/education/
  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 including a record of disposal
- The school's 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

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations
Environment Agency web site
Introduction
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
The Waste Electrical and Electronic Equipment Regulations 2013
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner website
https://ico.org.uk/
Data Protection Act – data protection guide, including the 8 principles
https://ico.org.uk/for-organisations/education/

PC Disposal – SITSS Information
http://www.thegrid.org.uk/info/traded/sitss/services/computer_management/pc_disposal

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 how to behave responsible online.

Managing e-mail

- The school gives all staff and Trustees their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- Staff & Trustees should use their school email for all professional communication
- 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 or the LA'. 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
- 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 students have their own school-issued account
- All pupil e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour 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 or upsetting e-mail
- Staff must inform (the e-safety co-ordinator or line manager) if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the Computing Programme of Study
- 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**

- 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
- School e-mail is not to be used for personal advertising
- Wherever possible staff should send attachments using OneDrive as this will ensure that the contents of the attachment are encrypted across the network.

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
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

e-mailing Personal, Sensitive, confidential or Classified Information

- Where your conclusion is that e-mail must be used to transmit such data:
-

  Either:

  Use Schoolsfx, Hertsfx or Hertfordshire's web-based Secure File Exchange portal that enables schools to send and receive confidential files securely
  http://www.thegrid.org.uk/eservices/schoolsfx.shtml

  Or:
  Obtain express consent from your manager to provide the information by e-mail and exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

  - Encrypt and password protect. See http://www.thegrid.org.uk/info/dataprotection/#securedata
  - 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 person whose details you have been unable to separately verify (usually by phone)
    - Send the information in a password protected document via the One Drive service.
    - 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

Pupils with additional needs
The school endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the schools' e-safety rules.

However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.
Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children and young people.

e-Safety

e-Safety Roles and Responsibilities
As e-safety is an important aspect of strategic leadership within the school, the Head and Trustees have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-safety co-ordinator in this school is *Toby Eager-Wright* who 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 e-safety co-ordinator to keep abreast of current issues and guidance through organisations such as Herts LA, Herts for Learning Ltd, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Trustees are updated by the Head/ e-safety co-ordinator and all Trustees 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, Trustees, 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 PSHCE.

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

- The school has a framework for teaching internet skills in lessons The school provides opportunities within a range of curriculum areas to teach about e-safety
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the e-safety 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, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate 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 Cybermentors, 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 Computing curriculum

e-Safety Skills Development for Staff
- Our staff receive regular information and training on e-safety and how they can promote the 'Stay Safe' online messages in the form of staff briefings and training sessions
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community (see e-safety Co-ordinator)
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

Managing the School e-Safety Messages
- We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used
- The e-safety policy will be introduced to the pupils at the start of each school year
- e-safety posters will be prominently displayed
- The key e-safety advice will be promoted widely through school displays, newsletters, class activities and so on
- We will participate in Safer Internet Day every February.

Incident Reporting, e-Safety 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 relevant responsible person or e-safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Information Asset Owner.

e-Safety Incident Log
Keeping an incident log can be a good way of monitoring what is happening and identify trends or specific concerns.

'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 may also need to be recorded elsewhere

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

This can be downloaded https://www.thegrid.org.uk/eservices/safety/policies.shtml

Misuse and Infringements

Complaints

Complaints and/or issues relating to e-safety should be made to the e-safety co-ordinator or Headteacher. Incidents should be logged and the **Hertfordshire Flowcharts for Managing an e-safety 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 e-safety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the e-safety Co-ordinator. Depending on the seriousness of the offence, sanctions could include 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.

Responding to online safety incidents in schools
The following information has been developed by the HSCB e-safety subgroup and are designed to help schools successfully manage e-safety incidents.

Online safety incidents in school

To support schools with online safety incidents please see the suggestions and contact details below.

All Online Safety incidents should be recorded. The HFL model Online Safety Policy has exemplar incident logging and reporting forms. http://www.thegrid.org.uk/eservices/safety/policies.shtml

Online safety incident reporting form
Online safety Incident Record for Staff Completion
Online Safety Incident Log

If you have any concerns about HGfL Filtered Internet Service or wish to have a website blocked please refer to HICS (Hertfordshire Internet and Connectivity Service)

https://www.hertsforlearning.co.uk/business-services/ict-services/hertfordshire-internet-and-connectivity-service-hics

If the incident involves an illegal activity such as:

- Downloading or viewing child pornography
- Passing onto others images or videos containing child pornography
- Inciting racial or religious hatred
- Promoting illegal acts

Where possible, confiscate any laptop or mobile device and if related to the school network disable the account.

Inform the police and follow advice given.

If the alleged perpetrator is an adult working with children, the LADO threshold guidance should be consulted and consideration given to a referral to the LADO.

Consider a child protection referral to children's services, if the child is not at immediate risk the school can seek advice from the consultation hub by ringing 01438 737511.

HFL Wellbeing advisers are also available to offer advice and in school support - contact 01438 844819

If the incident involves a non-illegal activity where pupils are involved such as:

- Using another person's user name and password
- Accessing a website which is against school policy

- Using mobile phones in non-designated areas
- Using technology to upset or bully (in some cases this can be illegal)

Review the incident and identify pupils involved

- Follow the school disciplinary procedure
- Inform parents/carers as appropriate
- Review school policies / procedure to develop best practice
- Put in place in- school support for pupils from e.g. class teacher, online safety co ordinator, Senior Leader, DSP, school PCSO
- Seek support of HfL Wellbeing advisers if appropriate contact 01438 844819

Useful references relating to sexting concerns:

Sexting in schools and colleges: Responding to incidents and safeguarding young people
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609874/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf

NSPCC Sexting guidance for schools
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/sexting-advice-professionals/

Internet Access

Managing the Internet

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity
- Staff will preview any recommended sites, online services, software and apps before use
- Searching for images through open search engines is discouraged when working with pupils
- If Internet research is set for Prep, 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

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience
- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application
- On-line gambling or gaming is not allowed

It is at the Headteacher's discretion as to 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 HICS web filtering service. For further information relating to filtering please go to http://www.thegrid.org.uk/eservices/safety/filtered.shtml
- Our school also employs some additional web-filtering which is the responsibility of the Network Manager
- Monk's Walk School 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 Co-ordinator or teacher as appropriate
- It is the responsibility of the school, by delegation to the network manager, 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 not the school's responsibility nor the network manager's 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 ***(technician/teacher)*** 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/technician/ICT subject leader)***
- If there are any issues related to viruses or anti-virus software, the network manager should be informed (Tel 244)

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 and online games websites to pupils within school
- All pupils are advised to be cautious about the information given by others on such websites, 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 websites 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 websites 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 their online profiles to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Our pupils are asked to report any incidents of Cyberbullying to the school
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other 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

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting e-safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss e-safety with parents/carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school e-safety policy by parent forums and the school council
- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (eg, on school website)
- Parents/carers are expected to sign a Home School agreement containing the following statement

    - **We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the school community or bring the school name into disrepute.**

- The school disseminates information to parents relating to e-safety where appropriate in the
    - Information evenings
    - Practical training sessions eg current e-safety issues
    - Posters
    - School website information

- Newsletter items
- Parent Mail
- Facebook/Twitter

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
- 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
- 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**
- **Never tell a child or colleague your password**
- **If you aware of a breach of security with your password or account inform the network manager immediately**
- Passwords must contain a minimum of six characters and be difficult to guess
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols
- User ID and passwords for staff and pupils who have left the school are disabled when they leave and removed within a year

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 private 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, learning platform and Management Information System log-in username. From ***Year 7*** they are also expected to use a personal password and keep it private
- Pupils are not allowed to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the 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 locked.
- Due consideration should be given when logging into the school learning platform, virtual learning environment or other online application to the browser/cache options (shared or private computer)
- In our school, all ICT password policies are the responsibility of the network 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 unauthorised access

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, and remove any portable media from computers when not attended.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- 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
- 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 encrypted with Bitlocker
- 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

Please refer to the document on the grid for guidance on How to Encrypt Files

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

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
- To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, eg. 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. HCC guidance can be found:
http://www.thegrid.org.uk/eservices/safety/research/index.shtml#safeuse

- 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
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Headteacher
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication

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
- on the school's learning platform or Virtual Learning Environment
- 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
- 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 or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.
- 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.
- 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.
- Only the ICT Manager or approved personnel have authority to upload to the internet.

For further information relating to issues associated with school websites and the safe use of images in Hertfordshire schools, see

http://www.thegrid.org.uk/schoolweb/safety/index.shtml
http://www.thegrid.org.uk/info/csf/policies/index.shtml#images

Storage of Images

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

- Pupils and staff are not permitted to use personal portable media for storage of images (eg, USB sticks) without the express permission of the Headteacher. The school offers alternative methods of transferring and storing images, and staff and students will receive training in their use.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource

CCTV

- The school uses CCTV for security and safety. The only people with access to this are **the network manager, the e-safety co-ordinator and the site manager.** Notification of CCTV use is displayed at the front of the school. Please refer to the hyperlink below for further guidance https://ico.org.uk/about-the-ico/consultations/cctv-code-of-practice-revised/

For further information relating to webcams and CCTV, please see
http://www.thegrid.org.uk/schoolweb/safety/webcams.shtml

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school
- All pupils are supervised by a member of staff when video conferencing
- The school keeps a record of video conferences, including date, time and participants
- Approval from the Headteacher is sought prior to all video conferences within school to end-points beyond the school
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences
- No part of any video conference is recorded in any medium without the written consent of those taking part

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS (previously CRB) checked
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

For further information and guidance relating to Video Conferencing, please see

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

School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity
- 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. You are responsible for the backup and restoration of any of your data that is not held on the school's network
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. 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
- 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. Staff should lock their machines when leaving them unattended
- 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, mobile devices 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 the school 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 children and young people. Mobile technologies such Smartphones, BlackBerrys, iPads, games players, are generally very familiar to children outside of school. 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 remain switched off and in their bags during the school day (including break and lunch times) Our mobile device restrictive use policy can be found on page 16 of our Behaviour for Learning Policy. http://www.monkswalk.herts.sch.uk/assets/Documents/02-About-Us/Policies/Behaviour-for-learning-Nov-2018-u.2019.pdf
- This technology may be used for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer
- 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 iPads 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
- Never use a hand-held mobile phone whilst driving a vehicle

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 HCC and 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 a member of SLT.

Removable Media
If storing or transferring personal, sensitive, confidential or classified information using Removable Media please consider the following;

- Always consider if an alternative solution already exists
- Only use recommended removable media
- Encrypt and password protect
- Store all removable media securely
- Removable media must be disposed of securely by your ICT support team

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
- Backup tapes should be encrypted by appropriate software
- Data must be backed up regularly
- Backup tapes/discs must be securely stored in a fireproof container
- Back up media stored off-site must be secure
- Newly installed Office Master PCs acting as servers and holding personal data should be encrypted, therefore password protecting data. At the moment SITSS do not encrypt servers, however Office PCs (including Office Master PCs) installed by SITSS are supplied with encryption software installed

Smile and Stay Safe Poster

SMILE and 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 may 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

Social Media including Facebook and Twitter
Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives. We control access to social media through the school network as follows:

- Our school uses Facebook and Twitter to communicate with parents and carers. The admin and data managers are responsible for all postings on these technologies and monitors responses from others
- Pupils are not permitted to use their mobile devices during the school day and therefore are not permitted to access their social media accounts through the school network whilst at school
- Staff, Trustees, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, Trustees, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, Trustees, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

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
- Ensure you remove portable media from your computer when it is left unattended
- 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 logoff 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, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or HCC 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.

Writing and Reviewing this Policy

Staff and Pupil Involvement in Policy Creation

- Staff, Trustees and pupils will be involved in making/ reviewing the Policy for ICT Acceptable Use through staff focus groups, parent forums and the school council.

Review Procedure

- There will be on-going opportunities for staff to discuss with the e-Safety co-ordinator any e-safety issue that concerns them
- There will be on-going opportunities for staff to discuss with the safety Co-ordinator any issue of data security that concerns them
- This policy will be reviewed every (24) months and consideration will be 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 Headteacher and SLT on May 20, 2019

Further Help and Support

Your organisation has a legal obligation to protect sensitive information under the Data Protection Act 2018. For more information visit the website of the Information Commissioner's Office https://ico.org.uk/

- Advice on e-safety - http://www.thegrid.org.uk/eservices/safety/index.shtml
- Further guidance - http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata
- School's toolkit is available - Record Management Society website – http://www.rms-gb.org.uk/resources/848
- Test your online safety skills http://www.getsafeonline.org
- Data Protection Team – email - data.protection@hertfordshire.gov.uk
- Information Commissioner's Office – www.ico.org.uk

- Cloud (Educational Apps) Software Services and the Data Protection Act – Departmental advice for local authorities, school leaders, school staff and governing bodies, October 2014. This is an advice and information document issued by the Department for Education. The advice is non-statutory, and has been produced to help recipients understand some of the key principles and their obligations and duties in relation to the Data Protection Act 1998 (the DPA), particularly when considering moving some or all of their software services to internet-based "cloud" service provision –

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/404098/Cloud-services-software-dept-advice-Feb_15.pdf

For additional help, email school.ictsupport@education.gsi.gov.uk

Current Legislation

Acts Relating to Monitoring of Staff e-Mail:

Data Protection Act 2018
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.legislation.gov.uk/ukpga/2018/12/contents

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 e-Safety

Racial and Religious Hatred Act 2006
It 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.

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 the 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
https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

Counter-Terrorism and Security Act 2019 (Prevent), Anti-Radicalisation & Counter-Extremism Guidance

https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services

Appendix

This Policy in Brief can be issued to visitors, laminated and posted at workstations or used as appropriate by the school. Schools will need to customise to suit local arrangements.

School Policy in Brief

- At this school we have an Acceptable Use policy which is reviewed at least annually, which all staff sign. Copies are kept on file. We use the LA model policy.
- ICT Acceptable Use Agreements are signed by all Staff/Trustees/Students/Visitors. We use the LA model agreements.
- Safe Handling of Data Guidance documents are issued to all members of the school who have access to sensitive or personal data.

Protected and Restricted material must be encrypted if the material is to be removed from the school.

- At this school we encrypt flash drives/use automatically encrypted flash drives for this purpose and limit such data removal.
- At this school we use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- At this school we follow LA guidelines for the transfer of any other internal data transfer, using Outlook secure export to Local Authority Pupil Database.

Sensitive or personal material must be held in a lockable storage area or cabinet if in an un-encrypted format (such as paper)

- At this school we store such material in lockable storage cabinets in a lockable storage area.
- At this school all servers are in lockable locations and managed by CRB-checked staff.
- At this school we use follow LA back-up procedures and lock the tapes in a secure cabinet. Back-ups are encrypted. No back-up tapes leave the site on mobile devices.
- At this school we use protocol for disaster recovery on our admin server.

Disposal: Sensitive or personal material electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.

- At this school we use the Authority's recommended current disposal firm for disposal of system hard drives where any protected or restricted data has been held.
- At this school paper based sensitive information is shredded, using cross cut shredders.
- At this school we are using secure file deletion software.
- Laptops used by staff at home (loaned by the school) where used for any protected data are brought in and disposed of through the same procedure. From 2009 all laptops have been set-up with laptop hardrive encryption.
- SuperUsers with access to setting-up usernames and passwords which enable users to access data systems eg for email, network access, SLG and Learning Platform access are controlled by the LA processes, supported by the LA ICT Support Service.
- Security policies are reviewed and staff updated at least annually and staff know who to report any incidents where data protection may have been compromised. Staff have guidance documentation.