Policy Name	Computing Policy including Data Protection
This Review Date	July 2019
Next Review Due	July 2022
Cycle	3 years
Ratified by Full Governing Body on	July 2019
Policy will be published	website

At Woolenwick Juniors, Computing is an integral part of daily life, with all in our community using Computing technology safely to enjoy and achieve, to contribute and prosper and to keep healthy.

AIMS

In our school we aim to:

- ensure staff and pupils are increasingly confident, creative, independent and safe users of computing technology;
- use computing technology effectively to motivate and inspire pupils and raise standards;
- develop an appreciation of the use of computing technology in the context of the wider world;
- provide continuity and progression in all of the strands of the Computing National Curriculum;
- develop Computing skills through cross curriculum contexts;
- develop an awareness, understanding and use of the ESD technologies available within our ECO school.
- care for and respect equipment.

INTRODUCTION

Computing 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 the 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 lifelong learning and employment.

Computing comprises a variety of systems that handle and allow the communication of electronically retrievable information. In order to prepare children for the digital age, Computing now includes the use of laptops, tablets, programmable robots, sound recorders, DVD machines, CD players, calculators, digital cameras, video cameras, voting systems and sensors. Communication tools include fax, TV, Internet, e-mail, blogging and the radio station.

We believe that the pupils of Woolenwick Junior School must be able to become digitally literate and be able to use, express themselves and develop their ideas through information and communication technology. To enable pupils to prepare for this, we believe that all pupils must have equal and appropriate access to Computing resources.

ROLES AND RESPONSIBILITIES

The Role of the Headteacher

The overall responsibility for the use of Computing technology rests with the Headteacher. The Headteacher, in consultation with the subject leader, technician and staff:

- ensures the Computing curriculum is adequately resourced by regular funding;
- ensures that Computing is used in a way to achieve the aims and objectives of the school;
- provides opportunities for the Computing Leader to monitor plans, assessment and lessons.

The Role of the Computing Subject Leader

The designated teacher should:

- ensure the development of a scheme of work for the Computing curriculum. This will develop the pre-requisites for the use of computing across the curriculum and as a discrete subject;
- monitor planning and assessment and feed concerns back to the Headteacher;
- observe lessons and support the development of Computing teaching;
- promote the integration of Computing within appropriate teaching and learning activities;
- develop and monitor the contributions of subjects to its cross-curricular use;
- identify appropriate resources to meet the needs of the Computing curriculum;
- encourages and supports colleagues in raising awareness of the potential of Computing;
- act as a contact point between the school and support agencies;
- provide limited technical expertise, drawing on the facilities of technicians or network managers where possible;
- inform staff of new developments in the curriculum and feedback on best practice in Computing;
- co-ordinate the evaluation and review of the school's Computing policy, including acceptable use, safety and data security.

The Role of Other Subject Leaders

There is a clear emphasis in the National Curriculum on teaching Computing across the curriculum in context. Subject leaders should plan where Computing should be used in their subject schemes of work. The Computing subject leader will offer support and advice when requested.

The Role of Class Teachers

Even though whole school co-ordination and support is essential to the development of computing capabilities, it remains the responsibility of each teacher to plan appropriate Computing activities and assist the co-ordinator in the monitoring and recording of pupil progress in Computing.

Special Needs and Equal Opportunities

The school recognises the advantages of the use of Computing technology by children with special educational needs. Targets on children's ISPs are supported through the use of specific programs e.g. Rapid Write. In addition to this our school uses Computing technology to:

- increase access to the curriculum;

- improve language skills, especially EAL children.
- Positive images of computer use by children of both sexes are promoted.
- The school promotes equal opportunities for computer usage.

Teaching and Learning

- Where possible pupils will be encouraged to train and assist their peers.
- Each pupil will be introduced to the basic Computing skills required to operate effectively with the technologies in this school.
- Pupils will use Computing to support curriculum areas including literacy, numeracy, core and foundation subjects.
- Staff will use a range of teaching styles with Computing i.e. whole class, small group and individual use of Computing equipment.
- Provision will be made for differentiation in order to develop the potential of pupils who are more capable in Computing such as same activity different outcome; same theme different levels of input; different paces of work and different groupings of children.
- The staff will meet regularly to monitor and evaluate current Computing practice within the school, including pupils' continuity and progress.

Assessment, Reporting and Recording

Formative assessment of Computing will take place throughout the teaching of individual Computing units using the Hertfordshire Primary Computing Scheme. Summative assessment will be carried out termly (through an integrated project) and will reflect the development of children's Computing capability. Clear learning objectives both in Computing and subject context will support the focus of assessed activities.

The Computing subject leader organises the collection of samples of Computing technology work, which are used in the school's Computing portfolio. This is maintained in order to obtain consistency across our school. It is updated by the Computing leader on a regular basis.

Monitoring, Evaluation and Review

The SLT monitor planning each term and provide feedback to teachers. This ensures the scheme of work is implemented. In addition to this, the Computing subject leader monitors teaching and children's' work on a rotational basis. The Governors are kept informed of the subject leader's work and any areas of concern they identify. There is a governor who has responsibility for Computing.

The scheme of work is reviewed and updated on annual basis, to ensure it reflects good practice. The scheme of work provides sufficient detail to ensure all children receive a consistent experience in Computing and includes links with e-Safety.

RESOURCE MANAGEMENT

Human

Staff meeting time will be allocated to support the development of Computing in the school when appropriate. This may include: training; whole school support in planning for Computing; the development of the Computing portfolio or sharing ideas of good practice.

Staff are encouraged to discuss their training needs with the subject leader and there is an audit of skills and understanding carried out when required.

Our staff have the advantage of using the Internet for their own professional development by access to national developments, educational materials and good curriculum practice.

Technical
Any faults with the computers are reported to the Computing leader and recorded in a fault book. The outside agency technician is then able to deal with the problems.

Hardware
The school intends to enhance the provision of Computing equipment whenever possible. A three-year Development Plan and an annual review of needs will be made so that a systematic updating of equipment is implemented.

Obsolete equipment is disposed of in accordance with County and ESD guidelines.

The following resources are available in the school: network computers, netbooks, iPads, ipods, Interactive whiteboards, laptops, calculators, DVD players, digital cameras, digi-blu cameras, FLIP cameras, sensor equipment, programmable control toys and equipment, stereos, stage lighting, weather station, web cam, fax machine, voice recorders, OHP's, laptops for teachers and the radio station.

Health and Safety
All equipment is checked annually under the Electricity at Work Regulation 1989. A detailed inventory is kept up to date by the Facilities Manager and ensures all equipment is checked. New equipment is added to the inventory on arrival.

Internet
The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. In addition, home school learning is encouraged via the use of interactive tools such as Matheletics and Marvellous Me.

*Please see '****Woolenwick Junior ICT and E-Safety Agreement****' for further detail on safety policy.* **Internet use will enhance learning**

The school Internet access will be designed expressly for pupil and staff use and will include filtering appropriate to the age of pupils.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be encouraged to discuss copyright and the ownership of information and images copied from the Internet.

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

At Woolenwick Junior 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 school and at home.

Children’s learning follows an age-related, comprehensive curriculum for e-safety that enables pupils to become safe and responsible users of new technologies.

School works closely with all families to help them ensure that their children use new technologies safely and responsibly both in and outside of school. Teachers, families and children are made aware of common risk encounters online including negative exposure to gaming and other forms of digital interaction. The school systematically reviews and develops e-safety procedures, including training of staff, to ensure that they have a positive impact on pupils’ knowledge and understanding on how to handle possible risks of content, contact and conduct when accessing the internet.

Woolenwick Junior holds 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 our 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.

This policy (for all staff, governors, visitors and pupils) is inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), 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, camera phones, PDAs and portable media players, etc.).

ICT (including the internet, email, laptops, digital cameras etc) is an important part of learning in Woolenwick Junior School. We expect all children to be safe and responsible when using any form of ICT. The school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials and that ICT lessons do include eSafety. However, the school cannot be held responsible for all the content of materials accessed through the internet. Therefore, parents/Carers are expected to read through the ‘**Woolenwick Junior ICT and E-Safety Agreement**’ highlighting online safety rules with their child and talk with them to ensure they understand their importance and what it means for them (and for you).

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: safeguarding, GDPR, health and safety, home–school agreement, behaviour, anti-bullying and PSHCE/RSE policies, E-Safety and ICT and Computing.

The Headteacher and Governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety co-ordinator in this school is XXXXXX (DPO). All breaches of this policy must be reported to the DPO. All breaches of this policy that may have put a child at risk must also be reported to the DSL XXXXXX. Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. If, however, they have any access to the school network and equipment then they must adhere to the school’s **online safety procedures and acceptable use agreements**. If an organisation doesn’t have a policy, then school can support them to get one in place.

Monitoring

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

Breach of Use

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

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, the HCC Disciplinary Procedure or Probationary Service.

Policy breaches may also lead to criminal or civil proceedings.

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

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, reference will be made to the school's behaviour policy.

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 as follows:

Gary Hawkins, Headteacher
Katie Corrigan – Deputy Headteacher
Justine Terry – PA to the Headteacher
Suzi Armstrong – Office Manager

- DPO
- IT Man

Who do you want in this list?

Please refer to the relevant section on Incident Reporting, eSafety Incident Log and Infringements in the school e-safety policy.

Data Security

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

- 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).
- Leadership have identified the Senior Information Risk Owner (SIRO) and Asset Information Owner(s) (AIO) 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 computing 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 computing 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.
- Anyone sending a confidential or sensitive fax or e-mail should notify the recipient before it is sent.

Relevant Responsible Persons

Senior members of staff should be familiar with information risks and the school's response. Previously called a Senior Information Risk Officer (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.

Protective Marking of Official Information

- Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them, in line with local business processes.
- There is no requirement to mark routine OFFICIAL information.
- Optional descriptors can be used to distinguish specific type of information.
- Use of descriptors is at an organisation's discretion.
- Existing information does not need to be remarked.

In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: '**OFFICIAL–SENSITIVE'**

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 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 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 and will be approved by the Governing Body:

- 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 e.g. waste, gift, sale
- Name of person and / 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 2006
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

Email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and how to behave responsible online.

Staff and governors should use a school email account for all official communication to ensure that children are protected through the traceability of all emails through the school email system. In addition, it is important that governors are protected against possible allegations of inappropriate contact with children. This is to help mitigate the chance of issues occurring and is an essential element of the safeguarding agenda.

Managing Email

The school gives all staff and Governors their own email 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 emails and avoids the risk of personal profile information being revealed.

Staff and Governors 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, email 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 email addresses

The school requires a standard disclaimer to be attached to all email 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 emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated line manager.

Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

Emails 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 email account as follows:

- Delete all emails of short-term value
- Organise email into folders and carry out frequent housekeeping on all folders and archives

Children will use a class/ group email address.

The forwarding of chain emails is not permitted in school.

All pupil email 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 email 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 email.

Staff must inform (the eSafety coordinator or line manager) if they receive an offensive email.

Pupils are introduced to email as part of the Computing Programme of Study.

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

Sending emails

- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section Emailing Personal or Confidential Information.
- Use your own school email account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of email 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 email is not to be used for personal advertising.

Receiving emails

- Check your email 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 email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.
- The automatic forwarding and deletion of emails is not allowed.

Emailing Personal or Confidential Information

Where your conclusion is that email 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 email and ***exercise caution when sending the email and always follow these checks before releasing the email:***

Encrypt and password protect. See
http://www.thegrid.org.uk/info/dataprotection/#securedata

- Verify the details, including accurate email address, of any intended recipient of the information.
- Verify (by phoning) the details of a requestor before responding to email requests for information.
- Do not copy or forward the email 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 as an encrypted document **attached** to an email.
- 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 email.
- Request confirmation of safe receipt.

MISUSE AND INFRINGEMENTS

Complaints

Complaints and/or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher. 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.

Passwords

- Always use your own personal passwords to access computer-based services.
- Make sure you enter your personal passwords each time you log on. 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 Computing 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.
- User ID and passwords for staff and pupils who have left the School are removed from the system within ***2 weeks.***

If you think your password may have been compromised or someone else has become aware of your password report this to your Computing 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.

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 school networks, MIS systems 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 ***7.00pm***.

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 unauthorized 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 labelling.

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.
- 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.
- 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 server.
- Always keep servers in a 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.
- Data must be backed up regularly.
- Back up media stored off-site must be secure.
- Remote back ups should be automatically securely encrypted. SITSS provide an encrypted remote back up service. Please contact the SITSS helpdesk for further information – 01438 844777.
- 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.

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 Computing equipment or your own PC.
- Do not allow any unauthorized person to use school Computing 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 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 Computing technology 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. *Hertfordshire Business Services, RM and RecycleIT all offer this service.*

Telephone Services

You may make or receive personal telephone calls provided:

1. They are of importance, 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. Permission has been sought from a member of the SLT

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.

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.

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 SIRO/AIO any issue of data security that concerns them.

This policy will be reviewed every three 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.

Appendix

Information Risk Actions Form
(could be included in the 'Register of Information Assets – Appendix 3)
Add your own one Gary or use this as a sample?

Information Asset	Information Asset Owner	Protective Marking	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk