MANOR HOUSE
BOOKHAM
EST.1920

Manor House School Acceptable Use and Computer Technology Policy (Including e-safety)

CONTENTS

Introduction

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

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

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, is not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

At ***Manor House School,*** we understand the responsibility to educate our pupils on eSafety Issues, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and 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 our 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, governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet, technologies provided by the school (such as PCs, iPads, 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, iPads, mobile phones and other mobile devices).

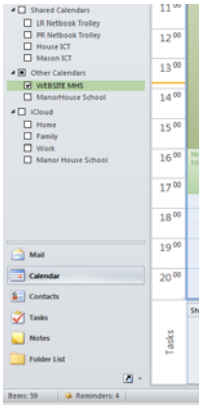
ICT Provision

To help gain the most benefit from the ICT resources within school the following regulations are to be followed by both staff and pupils.

This policy should be read in conjunction with the iPad acceptable use policy.

Pupils have use of computers in two ICT suites, a Language Laboratory and the library, in addition to computers in other areas and some classrooms. There is a phased introduction of 1:1 iPads into the Senior department (See the iPad Acceptable Use Policy).

Booking of ICT Suites



This is co-ordinated by the ICT Technician. Staff are to book ICT facilities on the appropriate booking form on Outlook. This is accessed via a link of the Outlook calendar (See Screen shot on the right)

Printing

Printing costs are high and should be kept to the minimum possible. All appropriate documents are to be named in a footer with initials and surname. (For exams this should include Name, Candidate Number and Centre Number.)

If prints do not appear at the expected printer immediately check the destination printer that was chosen or the status of the printer itself. This good practice should form part of any teaching in the ICT suites and hence should always be reinforced to pupils.

Printing is released from copiers by entering a staff specific code. If printing from an iPad then these print jobs are released by scanning a QR code at the relevant printer with the iPad Printing App.

Monitoring

The ICT technician or Deputy Head may inspect any ICT equipment owned by the school at any time without prior notice.

The ICT technician may monitor, intercept, access, inspect, record and disclose e-mails, internet/intranet use and any other electronic communications (data, voice, video or

image) involving 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 1998, 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 monitoring, surveillance or investigative activities are conducted by authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

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

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

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 and can affect their Probationary Period.

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 passwords), 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: the ICT technician and Deputy Head.

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

Acceptable Use Agreement: Pupils - Junior

Junior Pupil Acceptable Use Agreement / eSafety Rules

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send photos of me unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.

- I know that my use of ICT can be checked and my parent/guardian contacted if a member of school staff is concerned about my safety.
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher.
- I will not view unsuitable material on websites.
- I will not send any inappropriate material or post pictures of others on external sites without their permission.
- I will not give out personal information about myself when using a computer.
- I will not access chat rooms or instant messaging services in school or services such as facebook.
- I will also read and sign the iPad user policy if my year group is allowed to use iPads.

SAFETY WARNING: When inputting at the keyboard, a person should keep the shoulders relaxed with the elbows at the side, with the keyboard and mouse positioned so that reaching is not necessary. The chair height and keyboard tray should be adjusted so that the wrists are straight, and the wrists should not be rested on sharp table edges. Wrist or palm rests should not be used while typing. iPads should not be at an angle of more than 30 degrees to the horizontal when typing directly on them.

Acceptable Use Agreement: Staff, Governors 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 Deputy Head.

- I will only use the school's email / Internet and any related technologies for professional purposes or for uses deemed acceptable by the Headmistress or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number (unless needed on a school trip), personal e-mail address, personal Twitter account, or any other social media link, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on Schoolbase) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headmistress or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g on a password secured laptop or memory stick.

- I will not install any hardware or software without permission of the ICT technician, on networked machines.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member.
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headmistress.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headmistress or Deputy Head. I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional role or that of others into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will not use the school's internet for financial gain, political purposes or advertising.
- I will not attempt to gain unauthorised access to the Manor House School network or to any other computer system found on the Internet.
- I will not spend an unreasonable amount of time during the working day using school computers for personal use, nor will I use computers in communal areas for personal purposes at any time when they might be needed by others for work purposes.
- I will lock the screen or log out of a computer when I leave my desk.
- I will also read and sign the iPad acceptable use policy.

SAFETY WARNING: When inputting at the keyboard, a person should keep the shoulders relaxed with the elbows at the side, with the keyboard and mouse positioned so that reaching is not necessary. The chair height and keyboard tray should be adjusted so that the wrists are straight, and the wrists should not be rested on sharp table edges. Wrist or palm rests should not be used while typing. iPads should not be at an angle of more than 30 degrees to the horizontal when typing directly on them.

Staff Professional Responsibilities

Below is 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.

Health and Safety

Normal School Health and Safety Policy must be followed when dealing with all ICT resources.

Additionally, the following must be complied with:

- Rules for the use of ICT facilities are displayed prominently within school ICT suites and must be followed by all staff and pupils.
- Equipment must not be moved from its authorised location without the authority of the ICT Technician
- Repairs must not be undertaken except by the ICT Technician, ICT teaching Staff or ICT contractors employed by the school
- School bags should be kept out of walk-ways to prevent tripping
- Food and drink are not to be taken into any of the ICT Suites at any time
- Workstation areas must be kept clear of all clutter as computers require a clear airflow to assist internal cooling
- Safety and comfort guides for those spending long periods at workstations are included in Appendix 1
- Procedures for good practice whilst using workstations will be communicated, by the Head of Computing, to both pupils and staff following the guidance published by the HSE. This guidance is published as part of the Computing department handbook and is held as hard copy in the Computing department.
- All members of the school community should avoid looking directly into the beams of light from classroom projectors
- Devices, such as projectors, will be switched off after use to avoid damage through overheating and to save energy.

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. (This is set to be automatically checked)
- Never interfere with any anti-virus software installed on school ICT equipment.
- If you suspect there may be a virus on any school ICT equipment, stop using the

equipment and contact ICT support immediately. The ICT technician will advise you what actions to take and be responsible for advising others that need to know.

Data Security

Security

- The school gives relevant staff access to its Management Information System (Schoolbase), 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 should 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.

Relevant Responsible Persons

Senior members of staff should be familiar with information risks and the school's response. The Data protection officer (Director of Finance and Operations) and e-safety Officer (Deputy Head) have 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 pupils and staff; such as assessment records, medical information and special educational needs data. The Data Protection Officer 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 the Data Protection Officer is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

Handling of secured data is everyone's responsibility – whether you 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.

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 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.
- 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.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper, using formal salutations for recipient

and sender.

- The school gives all senior pupils their own e-mail account to use for school. Pupils may only use this school approved account on the school system 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

- The following pupils have their own individual school issued e-mail accounts ***(Year 7-Year 11).***

- The forwarding of chain emails is not permitted in school.

- 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 eSafety 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.

- All e-mail traffic is automatically monitored by the Bloxx system and will report unacceptable language or image use.

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, or send e-mails via Schoolbase to parents.

- 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 .

Receiving e-mails

- Check your e-mail regularly (at least once a day).
- Activate your 'out-of-office' notification when away for extended periods.
- Never open attachments from an untrusted source; Consult the ICT Technician first.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.
- The automatic forwarding and deletion of e-mails is not allowed.

---

e-mailing Personal, Sensitive, Confidential or Classified Information

- Where your conclusion is that e-mail must be used to transmit such data:
  - Obtain express consent from your manager to provide the information by e-mail
  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
    - 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 as an encrypted document **attached** to an e-mail
  - Provide the encryption key or password by a **separate** contact with the recipient(s)
  - Do not identify such information in the subject line of any e-mail
  - Request confirmation of safe receipt

Equal Opportunities

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 school's eSafety 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 eSafety issues.

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

eSafety

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Headmistress and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is *Michael Gates (Deputy Head)* who has been designated this role. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations, CEOP (Child Exploitation and Online Protection) and Childnet. The Head of Key Stage 4 will also co-ordinate the appropriate e-safety training for all staff.

Senior Management and Governors are updated by the Headmistress / eSafety co-ordinator and all Governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's Acceptable Use Agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

All staff are expected to partake in an online e-safety for teachers Annual Training, offered by E-Safety Support, for which certificates are awarded and placed in their personnel files. The Head of Key Stage 4 will co-ordinate this.

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is

essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching internet skills in Computing/ICT/PSHE lessons, this can be found in the relevant subject handbook.
- The school provides opportunities within a range of curriculum areas to teach about eSafety, which also includes visiting speakers.
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright, 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.
- Participate in Safer Internet Day

---

eSafety Skills Development for Staff

- Our staff receive regular information and training on eSafety and how they can promote the 'Stay Safe' online messages. All staff and Governors are expected to partake in an online e-safety for teachers Annual Training, offered by E-Safety Support, for which certificates are awarded and placed in their personnel files. (An optional parent version is also available)
- 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 eSafety and know what to do in the event of misuse of technology by any member of the school community (see eSafety Co-ordinator)

- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

Managing the School eSafety Messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.
- The eSafety policy will be introduced to the pupils at the start of each school year.
- eSafety posters will be prominently displayed.
- The key eSafety advice will be promoted widely through school displays, newsletters, class activities and so on.
- Website has current e-safety news available.

Incident Reporting, eSafety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access 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 Deputy Head.

eSafety Incident Log

Keeping an incident log can be a good way of monitoring what is happening and identify trends or specific concerns. Bloxx keeps logs of infringements are monitored byt eh ICT Technician and printed off and distributed when an issue arises..

Misuse and Infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headmistress. Incidents should be logged and the Manor House School procedure for complaints should be followed.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the

Headmistress or Deputy Head. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences

- Users are made aware of sanctions relating to the misuse or misconduct by in the school rules and staff handbook

Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internet use through the school network is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up by the Deputy Head.

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 homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Internet Use

- 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 Deputy Head's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- Our school also employs some additional web-filtering which is the responsibility of ***the ICT Technician***
- Manor House 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 coordinator or teacher as appropriate
- It is the responsibility of the ICT Technician, 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 ICT Technician to install or maintain virus protection on personal systems. All members of the school community are entitled to a copy of the School's virus programme as per the site license. A copy can be obtained from the ICT technician.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from ***(the Deputy Head/ICT technician)***
- If there are any issues related to viruses or anti-virus software, the ICT Technician should be informed in person, via email or phone call.

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 endeavours 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 Headmistress
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm
- Older pupils are also warned about phishing e-mails.

Parental Involvement

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

- 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 (e.g., on school website)

- The school disseminates information to parents relating to eSafety where appropriate in the form of;
    - Information evenings
    - Practical training sessions e.g. current eSafety issues
    - Posters
    - School website information
    - Newsletter items

Passwords and Password Security

Passwords

Please refer to the document, at the following link, 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 Deputy Head immediately**
- Passwords must contain a minimum of seven 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 removed from the system within ***24 hours*** of them leaving.

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 and Schoolbase log-in username. From ***Year 3*** 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.
- Staffare 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. The automatic log-off time for the school network is 15 minutes.
- Due consideration should be given when logging into Schoolbase or other online application to the browser/cache options (shared or private computer).
- In our school, all ICT password are to be changed every three months.
- See Guide to Setting Safe Passwords of central folder.

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 unauthorised access
- Regularly change generic passwords to avoid unauthorised access (Microsoft® advise every 42 days)

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

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

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 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, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

Safe Use of Images

Taking of Images and Film

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

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

- 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 Headmistress, 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 Deputy Head or Class Teacher
- Pupils and staff must have permission from the Headmistress before any image can be uploaded for publication

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing Pupils' 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, eg 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 usually 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 except in newspapers and with the consent of parents.

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

For further information relating to issues associated with school websites and the safe use of images, 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
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headmistress
- 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
- ***The ICT Technician*** has the responsibility of deleting the images when they are no longer required, or when the pupil has left the school

Webcams and CCTV [for when we have the CCTV installed]

- The school uses CCTV for security and safety. The only people with access to this are **the office staff.** Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school
- Webcams will not be used for broadcast on the internet without prior parental consent
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)
    - Webcams can be found ***(state where).*** Notification is given in this/these area(s) filmed by webcams by signage
    - Consent is sought from parents/carers and staff on joining the school, in the same way as for all images
- Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices

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

Video Conferencing

- Permission must be 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 Deputy Head is sought prior to all video conferences within

school to end-points beyond the school

- 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

http://www.thegrid.org.uk/learning/ict/technologies/videoconferencing/index.shtml

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

School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity.

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

- Do not allow any external 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.

- 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.

- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver, as must any user profiles.

- Privately owned ICT equipment should not be used on a school network unless connected via the wifi.

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

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

- All ICT equipment allocated to staff must be authorised by the Deputy Head who is 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 school's 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 the ICT Technician.

- 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, Blackberries, 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 while in school. If this is necessary from home then precautions should be made to hide the number from which you are calling.
- Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched off and all year groups except Year 11 must hand these in to the office.
- iPads and Laptops may be used for educational purposes, as mutually agreed with the Headmistress*, as long as an iPad acceptable use policy has been signed*
- 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.

Removable Media

If storing or transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section '**Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media**' - Page 33

- 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

- The servers are in a locked and secure environment
- The servers have limited access rights
- The servers are password protected and locked
- The existing servers have security software installed appropriate to the machine's specification
- Backup tapes are encrypted by appropriate software
- Data is backed up every day
- Backup tapes/discs are securely stored in a fireproof container off site
- Backup media stored off-site is secure

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Our school uses Facebook and Twitter to communicate with parents and carers. The Marketing Manager and Deputy Head are responsible for all postings on these technologies and monitor responses from others

- Pupils are not permitted to access their social media accounts whilst at school

- Staff, governors, 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, governors, 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, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

Staff Guidelines for Social Media Posting

- For data protection reasons, all social media postings should first be released on Manor House School's recognised social media accounts and then re-tweeted or re-posted on personal accounts. These accounts are Twitter: @ManorHseSchool and Facebook: /manorhousesch (unless otherwise notified).

- To increase the volume of social media messages, a named person in each department may be given access to our Twitter and Facebook accounts and take on responsibility (in addition to Marketing who retain overall responsibility) for posting out social media news for their department only.

- Only the nominated department representative can post news.

- The school operates an integrated marketing approach where possible when posting web and social media news by pre-scheduling items at specific times and linking to the news story on our website. This drives traffic to our website. Stand-alone social media does not replace the need for news articles. Major trips or events should still be submitted as news articles or press releases to Marketing. The function of a further social media resource is to get additional items or curricular activity on-line.

- The login and passwords are not to be shared with anyone else without prior permission from the Marketing Department.

- If you are unsure as to the content or relevance of the post, then please refer to the Marketing Department.

- Posts must go on both FB and Twitter accounts to keep communication consistent and ensure we reach parents who use only one medium.

- When posting, be aware of optimum viewing times on social media for maximum exposure; late afternoon/early evening, after morning school run or around lunchtime.

Permitted Message content

- Social media content should be centred on our six school brand values which are:

- Academically strong

- Understanding Individuality

- Supportive and Nurturing

- Smaller but mighty
- Creative and expressive
- Friendly and welcoming

Permitted Photography

- Photographs must show girls in school uniform wherever possible to reinforce the school brand identity.
- Representatives must be aware of omitting girls whose parents have not given permission for social media usage. Please familiarise yourself with the latest data protection declined usage which can be found at: S:\OFFICE\Data protection\Data Protection - declined use\Declined Use of Data and Photographic - Date – with photos.
- Staff data protection must be considered. If staff are featured in photographs, the representative must check that permission has been provided before posting. However, brand guidelines stipulate that we show girls and the school, not staff, wherever possible.
- Photographs should reflect the imagery guidelines stipulated on page 17 of the school brand guidelines. (please refer to Marketing for a copy).

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, do not click on unsafe links in e-mails.

- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing of the data.

Telephone Services

- You may make or receive personal telephone calls provided:

1. They are infrequent, kept as brief as possible and do not cause annoyance to others
2. They are not for profit or to premium rate services
3. They conform to this and other relevant school policies.

- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused
- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases
- Ensure that your incoming telephone calls can be handled at all times

Writing and Reviewing this Policy

Review Procedure

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

This policy will be reviewed and revised regularly 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 staff, Headmistress and governors on

Date: _____

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of in such a manner as to prevent any school data access on the redundant equipment.
- 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. If the storage media has failed it will be physically destroyed.
- 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

- 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 2006

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

Appendix 1

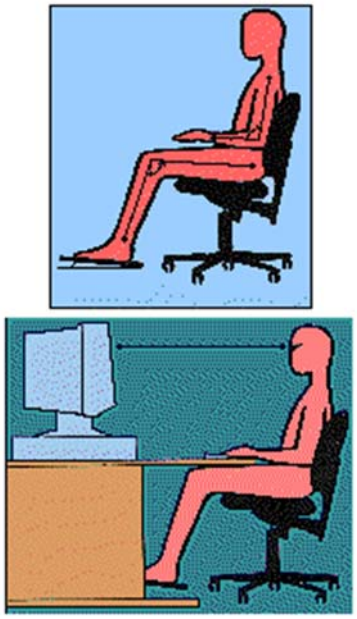
Summary for Good Seated Posture at the Computer

- A good posture is one in which you are comfortable and well supported by properly adjusted furniture. It reduces muscle strain and fatigue.

Comfortable viewing distance;

- shoulders relaxed
- elbows level with home row of keys and close to sides of body
- wrists straight
- ample leg room
- balanced, upright head position
- backrest supports the spine (natural "S" curvature)
- avoid pressure at the front edge of the seat
- feet firmly supported.

  Note: chairs for most keyboard activities should not have arm rests.



Adjusting your Furniture

For fixed height desks:

1. Chair height - adjust the chair so that your elbow tips are at the same level as the home row (ASDF) of keys.
2. Footstool - adjust the height so that your hips are slightly lower than your knees.

   Thighs parallel with the floor.

For adjustable height desks:

1. Chair height - adjust the chair so that your feet are flat on the floor and your hips are slightly lower than your knees.
2. Desk height - adjust the desk so that your elbow tips are at the same level as the home row (ASDF) of keys.

For both types of desks:

1. Lumbar support - adjust the height of the back rest to support the lumbar curve (small) of your back. To find your lumbar curve, hold your arms behind your back and comfortably clasp the opposite forearm near the elbow.
2. Seat depth - adjust the seat depth so that you are firmly supported by the back rest and can still fit 3 fingers between the front of your seat and the back of your legs.
3. Screen - adjust the top of the screen to the level of your eyes with the centre of the VDU screen no higher than 400mm above the work surface. Position the screen at a comfortable viewing distance usually between 400-550mm from the table front edge.
4. Document holder – if working from reference documents, the document holder is best located between the keyboard and the hard-drive. Alternatively to the side, but at the same level as the screen

---

Other Issues

Using a mouse

Prolonged use of a mouse can cause discomfort in the arms and shoulders.

- Use the mouse as close to the side of the keyboard as possible.
- Hold the mouse between your thumb and your third and fourth fingers. Your first and second fingers should rest lightly on the mouse buttons.
- Use the scroll button feature on the mouse and keep your second (middle) finger on it. This ensures correct positioning of the hand on the mouse.

Computer screens and eyesight problems

A complaint sometimes heard from keyboard operators is that looking at screens hurts their eyes or that the screens have caused them to need glasses. Screens can cause visual discomfort from glare or unwanted reflections on the screen, or from sitting at an incorrect distance from the screen, but they do not affect eyesight. When glasses are required it is because sitting at a fixed distance from the screen makes existing problems more noticeable.

- Users of VDU screens should have their eyes tested prior to starting work with VDUs and every two years afterwards if over the age of 40, or whenever problems are experienced.
- If you use glasses, single strength lenses are suggested. Using bi-focal or multi-focal lenses is not recommended.
- Ensure steps are taken to minimise glare.

Laptop or Notebook PCs

Laptop and notebook personal computers are useful for performing computing tasks when away from the office. Prolonged use of these devices is not advisable. The small size of the keyboard, and the position and small size of the screen do not enable users to adopt a good posture.

When using laptop for a prolonged period of time:-

- raise the screen on a platform to obtain the optimal viewing distance i.e. toolbar level with eyes when looking straight ahead.
- Use a separate detachable keyboard and mouse.

BORROWED FROM

(HTTP://WWW.SAFETY.UWA.EDU.AU/HEALTH-WELLBEING/PHYSICAL/ERGONOMICS/WORKSTATION)

Approved by SLT Sept 2018