



Appleton Primary School
eSafety Policy

Reviewed and Amended

Date 27.11.14

Reviewed and Amended

Date 2.3.16

CONTENTS

Introduction	1
Monitoring	3
Breaches.....	5
Incident Reporting.....	5
Acceptable Use Agreement: Pupils.....	6
Acceptable Use Agreement: Staff, Governors and Visitors	7
Computer Viruses.....	8
e-Mail	9
Managing e-Mail	9
e-mailing Personal, Sensitive, Confidential or Classified Information	10
Equal Opportunities	11
Pupils with Additional Needs	11
eSafety.....	12
eSafety - Roles and Responsibilities.....	12
eSafety in the Curriculum.....	12
eSafety Skills Development for Staff.....	13
Managing the School eSafety Messages.....	13
Incident Reporting, eSafety Incident Log & Infringements.....	14
Incident Reporting.....	14
eSafety Incident Log.....	14
Misuse and Infringements.....	14
eSafety Incidents.....	14
Internet Access.....	15
Managing the Internet	15
Internet Use	15
Managing Other Web 2 Technologies.....	17
Parental Involvement.....	18
Passwords and Password Security	19
Password.....	19

Password Security	19
Safe Use of Images	21
School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media.....	22
School ICT Equipment	22
Portable & Mobile ICT Equipment	23
Mobile Technologies	23
Social Media, including Facebook and Twitter	24
Telephone Services	25
Mobile Phones	25
Writing and Reviewing this Policy	26
Staff and Pupil Involvement in Policy Creation	26
Review Procedure	26
Current Legislation	27
Acts Relating to Monitoring of Staff eMail.....	27
Other Acts Relating to eSafety	27
Acts Relating to the Protection of Personal Data	29

Introduction

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

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

- Websites
- 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 with web functionality, including iPads
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

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

At Appleton C of E Primary 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 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 the school to use technology to benefit learners.

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

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices eg i pads, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, and other mobile devices).

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The *school* will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Please see our mobile phone policy for further details on this area of eSafety.

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. Authorised staff include the Computing Co-ordinator and our colleagues at 123ICT. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact the Computing co-ordinator. Any ICT authorised staff member will be happy to comply with this request.

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

ICT 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 ICT 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.

Acceptable use

	Staff & other adults			Pupils				
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Communication Technologies								
Mobile phones may be brought to school	X							
Use of mobile phones in lessons		X		X				
Use of mobile phones in social time		X		X				
Taking photos on cameras		X		X				
Use of other mobile devices eg tablets		X		X				
Use of personal email addresses in school, or on school network		X		X				
Use of school email for personal emails	X			X				
Use of messaging apps		X		X				
Use of social media		X		X				
Use of blogs	X						X	

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.

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.

Policy breaches may also lead to criminal or civil proceedings.

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

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

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

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Computing 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 Computing co-ordinator.

Please refer to the section [Incident Reporting, eSafety Incident Log & Infringements](#).

Acceptable Use Agreement: Pupils

Appleton Primary School

Acceptable Use Agreement for the Internet, Email and other Technologies

The school has Internet access and access to new technologies such as the learning platform to help our learning. These rules will keep everyone safe and help us to become responsible users.

- I will only use the internet when I have permission and I am supervised
- I will only use search engines and websites responsibly (AT KS1, I will only use websites that have been chosen by my teacher)
- I will not try to access any inappropriate websites, chat rooms, Instant Messaging or Social Networking sites in school
- I will not give anyone else my username or password to log onto the school computers and the learning platform
- I will only send emails to people that my teacher has approved
- My emails and communication on the learning platform will always be polite, use good English and not be used as a way to bully another child or adult
- I will not give out my address, home or mobile telephone number, email details or other personal information by email or through the learning platform
- I will tell my teacher straightaway if I come across any unsuitable pictures or information on the Internet by accident or if anything makes me feel uncomfortable or upset
- I will not bring USB pen drives, software or MP3 Players into school unless I have been given permission
- I will not download any files from the Internet in school unless I have permission
- I will not bring my mobile phone to school
- I understand that the school can check my computer file, my e-portfolio, any activity on the learning platform and any Internet sites that I have visited

I understand the rules above and agree to follow them. If I break any of these rules, I understand that:

1. My parent/carer may be informed
2. I might be banned from using the Internet, e-mail and Learning Platform for a period of time.
3. More serious action might be taken

Pupil Signature: _____ Date: _____

I have read and discussed the rules above with my child. I give permission for my child to use the Internet, e-mail and other technologies at school. We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or video that could upset or offend any member of the school community

Parent/Carer Signature: _____ Date: _____

Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor

Acceptable Use Agreement / Code of Conduct

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

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal or sensitive data taken off site must be encrypted.
- I will not leave laptops or other devices containing sensitive information in unsecured places such as cars.
- I will not install any hardware or software without permission of the ICT co-ordinator
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend 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 my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- 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.

User Signature

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

Signature Date

Full Name(printed)

Job title

Computer Viruses

- Never interfere with any anti-virus software (Sophos) installed on school ICT equipment that you use
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your Computing co-ordinator
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the Computing co-ordinator immediately. They will advise you what actions to take and be responsible for advising others that need to know

e-Mail

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. In order to achieve Computing level 4 or above, pupils must have experienced sending and receiving e-mails.

Managing e-Mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to 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- however we appreciate that the e-mail system is unwieldy and are currently investigating other options. For now, if you are not using your main school e-mail address it is your responsibility to ensure that your password is secure and to respond to any security breaches as appropriate.
- Parents and carers should be e-mailed via the office account, rather than using personal e-mail address, if possible.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher, or their line manager, if appropriate.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
 - Delete all e-mails of short-term value
 - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- The forwarding of chain letters is not permitted in school. However the school has arranged for chain letters which are causing anxiety to be forwarded to the office e-mail address (office.3850@appleton.oxon.sch.uk).

- All pupil e-mail users are expected to adhere to the generally accepted rules of etiquette 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. All attachments should be virus checked before opening.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail
- Staff must inform their line manager or the Computing coordinator if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the Computing Scheme of Work
- 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

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
 - Verify the details, including accurate e-mail address, of any intended recipient of the information
 - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
 - Do not copy or forward the e-mail to any more recipients than is absolutely necessary
 - Do not send the information to anyone 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 for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules.

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

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

eSafety

eSafety - Roles and Responsibilities

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

Senior Management and governors are updated by the Head/ eSafety coordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

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

eSafety in the Curriculum

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

- As Computing is embedded, where appropriate, throughout our curriculum, eSafety issues are discussed with classes as required. We also teach children about eSafety through PSHE lessons and whole school assemblies.
- The school provides opportunities within a range of curriculum areas to teach about eSafety
- 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 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 evaluate materials critically and learn good searching skills

through cross curricular teacher models, discussions and via the ICT curriculum

eSafety Skills Development for Staff

- Our staff receive regular information and training on eSafety and how they can promote the 'Stay Safe' online messages in the form of discussion and training during staff meetings
 - Details of the ongoing staff training programme can be found in the staff meeting minute book
 - 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 enclosed flowcharts)
 - All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas
-

Managing the School eSafety Messages

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

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 Computing coordinator. 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 also be reported to the ICT co-ordinator.

eSafety Incident Log

The Computing coordinator keeps an e-safety incident log, to record all incidents. All incidents should be reported so that they can be logged and tracked.

Misuse and Infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety coordinator or Headteacher. Incidents should be logged and reported to all staff and Governors and I23ICT (our ICT Support).

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
 - Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety coordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
 - Users are made aware of sanctions relating to the misuse or misconduct in staff training sessions (see minute book)
-

eSafety Incidents

All incidents will be reported to the Computing/eSafety coordinator to the headteacher/governors. All incidents will be taken seriously and investigated appropriately but sensitively. Staff and pupils are aware that evidence about eSafety incidents can be gathered from our internet service provider, internet firewall/filter, the server or from individual devices.

Internet Access

The internet is an open worldwide communication medium. 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 in school is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- The school 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 before use at KS1
 - We teach children how to search for images responsibly
 - If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher (at KS1). It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
 - All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
 - All users must observe copyright of materials from electronic resources
-

Internet Use

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

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

- Appleton Primary 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 school, by delegation to the network manager (123ICT), to ensure that anti-virus protection is installed and kept up-to-date on all school machines
- Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems.
- Pupils are not permitted to download programs or files on school based technologies
- If there are any issues related to viruses or anti-virus software, the network manager should be informed via the Computing coordinator

Managing Other Web 2 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 website or other systems approved by the Headteacher

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 and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy via school council and in our eSafety meetings.
- 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)
- Parents/carers are expected to sign an acceptable use agreement containing the following statement or similar
 - **We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or video that could upset or offend any member of the school community**
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
 - Information and celebration evenings
 - Practical training sessions e.g. How to adjust the Facebook privacy settings
 - Posters
 - School website
 - Newsletter items

Passwords and Password Security

Passwords

It is important that passwords for laptops/systems/flash drives etc are robust. It is each member of staff's responsibility to ensure that their passwords are secure. Passwords are strongest if they include numbers as well as letters.

- **Always use your own** personal passwords
- 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 are aware of a breach of security with your password or account inform the Computing coordinator immediately**
- User ID and passwords for staff and pupils who have left the school are removed from the system

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

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 eSafety Policy and Data Security
- Users are provided with an individual network, email and **Management Information System** (where appropriate) log-in username. From 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, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems, including ensuring that passwords

are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

- Due consideration should be given when logging into the school learning platform, virtual learning environment or other online application to the browser/cache options (shared or private computer)
- In our school, all ICT password policies are the responsibility of the Computing coordinator and all staff and pupils are expected to comply with the policies at all times

Safe Use of Images

- See our separate phone and camera policy for information on how we deal with images in school.

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

School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school 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
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:
 - maintaining control of the allocation and transfer within their Unit
 - recovering and returning equipment when no longer needed
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

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

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the ICT support team and fully licensed
- 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 as Smartphones, Blackberries, iPads, and 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)

See our separate phone and camera policy for details of how mobile phones are used in school.

Social Media, including Facebook and Twitter

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

- 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

Telephone Services

Mobile Phones

Please see our separate mobile phone and camera policy for details about mobile phone use in school.

Writing and Reviewing this Policy

Staff, Parent and Pupil Involvement in Policy Creation

- Staff, governors, parents and pupils have been involved in making/ reviewing the Policy for ICT Acceptable Use through school council, staff meetings, governor meetings and eSafety meetings with the PTA and parents.
-

Review Procedure

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

There will be on-going opportunities for staff to discuss with the Computing coordinator any issue of data security that concerns them

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

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

This policy has been read, amended and approved by the staff, head teacher and governors in December 2015

Current Legislation

Acts Relating to Monitoring of Staff eMail

Data Protection Act 1998

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

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

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

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

Regulation of Investigatory Powers Act 2000

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

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

Human Rights Act 1998

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

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

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

Sexual Offences Act 2003

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

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

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

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

The Computer Misuse Act 1990 (sections 1 – 3)

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

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

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

Malicious Communications Act 1988 (section 1)

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

Copyright, Design and Patents Act 1988

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

Public Order Act 1986 (sections 17 – 29)

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

Protection of Children Act 1978 (Section 1)

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

Obscene Publications Act 1959 and 1964

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

Protection from Harassment Act 1997

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

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

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

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

The Freedom of Information Act 2000

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