Lead School for CHANGE SCHOOLS PARTNERSHIP

E SAFETY

Guidance policies for ICT acceptable use.

Produced by: T Beeson

Date of issue: July 2013

Review date: July 2014

Guidance and Suggested Text

The following sections contain much **guidance** and **suggested statements** for schools to use in compiling their own school's Policy for ICT Acceptable Use. It is intended for staff and pupil use.

The Acceptable Use of ICT Agreement should be issued to the appropriate user for signature and collated by a designated member of staff.

Schools should ensure that all persons, including Governors and pupils, who join the establishment mid year are provided with the policy and agreement.

Introduction

ICT in the 21st Century is 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

- Learning Platforms and Virtual Learning Environments

- E-mail and Instant Messaging

- Chat Rooms and Social Networking

- Blogs and Wikis

- Podcasting

- Video Broadcasting

- Music Downloading

- Gaming

- Mobile/ Smart phones with text, video and/ or web functionality

- Other mobile devices with web functionality

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.

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

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling

should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Monitoring

Authorised ICT staff and SMT may inspect any ICT equipment owned or leased by the School at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please check with the SMT. 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.

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. Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

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

access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your E-safety officer and /or SMT.

Acceptable Use Agreement: Pupils - Primary

Primary Pupil Acceptable Use
Agreement / eSafety Rules

- I will use technologies with care and treat them with respect.
- 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 details such as my name, phone number or home address.
- I will not arrange to meet someone
- I will be responsible for my behaviour and follow the SMART IT rules.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

Name:

Class:

Signed:

Date:

Staff, Governor and Visitor

Acceptable Use Agreement / Code of Conduct

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

➢ 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, personal e-mail address and social networking identities to pupils.
➢ I will NOT communicate with children via social networking sites, e.g. Facebook
➢ I will not discuss school issues and reference the school's name via social networking sites.
➢ I will ensure that my privacy settings for a Social Network profile are set appropriately.
➢ I will only use the approved, secure e-mail system(s) for any school business.
➢ I will ensure that personal data 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 Headteacher .
➢ I will not install any hardware of software.
➢ 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 on a school device and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
➢ I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the e-safety officer or the 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.

This Acceptable Use Agreement is a summary of our eSafety Policy which is available in full from the school office

User Signature
I agree to follow this Acceptable Use Agreement and to support the safe and secure use of ICT throughout the school

Signature …….………………………………… Date ……………………

Full Name ……….…………………………..(printed)
Job title . . . .

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. memory stick, CD) must be checked for any viruses using school provided anti-virus software before using them

- Never interfere with any anti-virus software installed on school ICT equipment that you use

- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT leader/SMT immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. The school works in line with **The Privacy Notice – Data Protection Act 1998.**

Essex County Council provide our internet services which includes a filtering system.

Security

- The School gives relevant staff access to its Management Information System (Integris G2), with a unique ID and password

- It is the responsibility of everyone to keep passwords secure.

- Staff are aware of their responsibility when accessing school data

- Staff have been issued with the ICT Acceptable Use policy and the Acceptable Use Agreement

- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data

- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.

- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times

- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used

Anyone expecting a confidential/sensitive fax, should have warned the sender to notify before it is sent using the Safe Haven Fax procedure below:

Safe Haven Fax procedures

When sending personally identifiable information:

- ensure the recipient knows the fax is being sent.
- ensure the fax will be collected at the other end.
- send the front sheet through first.
- check that it has been received by the correct recipient.
- add the rest of the document to the fax.
- press the **redial** button.
- don't walk away while transmitting.
- wait for the original to process and remove it from the fax machine.
- wait for confirmation of successful transmission.
- confirm whether it is appropriate to fax to another colleague if they are not there to receive it.
- use only the minimum information and anonymise where possible

Disposal of redundant ICT 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. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen

- Disposal of any ICT equipment will conform to:

  The Waste Electrical and Electronic Equipment Regulations 2006

  The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal

- The school's disposal record will include:

  o Date item disposed of

  o Authorisation for disposal, including:

    ▪ verification of software licensing

    ▪ any personal data likely to be held on the storage media? *

  o How it was disposed of e.g. waste, gift, sale

o 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.

E mail

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

Managing e-mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.

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

- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account

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

- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

  – Delete all e-mails of short-term value
  – Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

- All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail

- Staff must inform (the eSafety co-ordinator/ line manager) if they receive an offensive e-mail

- Pupils are introduced to e-mail as part of the ICT 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.

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 **Error! Reference source not found.**

- Use your own school e-mail account so that you are clearly identified as the originator of a message

- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate

- School e-mail is not to be used for personal advertising

Receiving e-mails

- Check your e-mail regularly

- Activate your 'out-of-office' notification when away for extended periods

- Use the 'Delegation' facility within your e-mail software so that your e-mail can be handled by someone else while you are not at work (if available within your software)

- Never open attachments from an untrusted source; Consult your network manager first.

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

E-mailing personal, sensitive, confidential and or classified information.

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided wherever possible
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service

for sending e-mail containing sensitive information is not permitted

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

  - 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 anybody/person whose details you have been unable to separately verify (usually by phone)
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt

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

  - Essex Police

  - District and Borough Councils within Essex County Council

  - Essex NHS Trusts

Equal Opportunities

Pupils with additional needs

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

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

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

E-safety

e-safety 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 officer in this school is **Toni Beeson** who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety officer to keep abreast of current issues and guidance through organisations such ECC, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ e-Safety officer 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.

E-safety 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 provides opportunities within a range of curriculum areas to teach about eSafety

- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum

- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them

- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities

- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button

Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

E-safety skills development for staff

- Our staff receive regular information and training on eSafety issues in the form of PDMs and regular updates via The Notley Green IT Curriculum Development blog

- New staff receive information on the school's acceptable use policy as part of their induction

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see

enclosed flowchart)

- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas.

Managing the school's e-safety 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

- children will take part in regular e-safety workshops which are age appropriate and led by the e-safety officer.

Incident Reporting, e-safety incident log and 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 SMT and/or e-safety officer. Additionally, all security breaches, lost/stolen equipment or data (including remote access passwords), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported also.

e-safety incident log

Details of ALL e-safety incidents must be reported to the e-safety officer, where the incident log will be completed and sufficient evidence will be used to support this. SEE APPENDIX Incident log. This will be monitored termly by the Head teacher. Where bullying or racism are also involved, this will need to be recorded elsewhere as well.

Misuse and infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety officer or Headteacher. Incidents should be logged and the **Flowchart for Managing an eSafety Incident** should be followed.

Inappropriate Material

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

Internet access
Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- The school maintains students who will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology

- Staff will preview any recommended sites before use

- Raw image searches are discouraged when working with pupils

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research

- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources

- All users must observe copyright of materials from electronic resources

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience

- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog

- On-line gambling or gaming is not allowed

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

Infrastructure

School internet access is controlled through the LA's web filtering service.

- School name) 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 or social networking sites

- 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, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines

- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the ICT leader for a safety check first

- Pupils and staff are not permitted to download programs or files on school based technologies without seeking permission first from ICT leader/ Technical Support .

If there are any issues related to viruses or anti-virus software, the network manager should be informed.

Managing other web technologies (including social networking sites)

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

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

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are

- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online

- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)

- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals

- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online

- Our pupils are asked to report any incidents of bullying to the school

- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using our Frog VLE 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 also 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 related to ICT and associated risks.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school

- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)

    - Parents/ carers are expected to sign a Home School agreement.

- The school disseminates information to parents relating to eSafety where appropriate in the form of;

    - Information and celebration evenings
    - Posters
    - Website/ VLE postings
    - Newsletter items

Passwords and Password Security
Passwords

- Always use your own personal passwords to access computer based services

- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures

- Staff should change temporary passwords at first logon

- Change passwords whenever there is any indication of possible system or password compromise

- Do not record passwords or encryption keys on paper or in an unprotected file

- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished

- Passwords must contain a minimum of six characters and be difficult to guess

- 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 ICT support team.

Password Security

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

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security

- Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) log-in username. Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others

- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems 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.

- In our school, all ICT password policies are the responsibility of **the Headteacher** and all staff and pupils are expected to comply with the policies at all times.

Zombie Accounts

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

- Ensure that all user accounts are disabled once the member of the school has left

- Prompt action on disabling accounts will prevent unauthorized access

- Regularly change generic passwords to avoid unauthorized access (Microsoft© advise every 42 days)

Further advice available http://www.itgovernance.co.uk/

Personal or sensitive information

Protecting personal, sensitive, confidential and classified information.

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

- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access

- 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.

Remote Access

- You are responsible for all activity via your remote access facility

- Only use equipment with an appropriate level of security for remote access

- To prevent unauthorised access to School systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone

- Select PINs to ensure that they are not easily guessed, 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

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 Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device

- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupil's device

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

- on the school's Learning Platform

- in the school prospectus and other printed publications that the school may produce for promotional purposes

- recorded/ transmitted on a video or webcam

- in display material that may be used in the school's communal areas in display material that may be used in external areas, i.e. exhibition promoting the school

- general media appearances, e.g. 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, e.g. divorce of parents, custody issues, etc.

- Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

- Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

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

Webcams and CCTV

The school uses CCTV for security and safety. The only people with access to this are The Site Manager. Notification of CCTV use is displayed at the front of the school.

- We do not use publicly accessible webcams in school

- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults

- 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 on the classroom laptop*).*
  - Consent is sought from parents/carers and staff on joining the school, in the same way as for all images

Video Conferencing
- Permission is sought from parents and carers if their children are involved in video conferences

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school

- All pupils are supervised by a member of staff when video conferencing

- All pupils are supervised by a member of staff when video conferencing with end-points beyond the school

- The school keeps a record of video conferences, including date, time and participants.

- Approval from the Headteacher is sought prior to all video conferences within school

- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences

- No part of any video conference is recorded in any medium without the written consent of those taking part

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be 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.

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

School ICT Equipment
- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you

- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory

- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities if available

- Ensure that all ICT equipment that you use is kept physically secure

- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990

- It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive

- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted

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

- Privately owned ICT equipment should not be used on a school network

- On termination of employment, resignation or transfer, return all ICT equipment to the Headteacher. 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 technical support team. They are responsible for:

    o   maintaining control of the allocation and transfer within their Unit
    o   recovering and returning equipment when no longer needed

Portable & Mobile ICT Equipment

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

- All activities carried out on School systems and hardware will be monitored in accordance with the general policy

- Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey

- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis

- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades

- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support

- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight

- Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device

- Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time.   At all times the device must be switched onto silent

- This technology may be used, however for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer

- The school is not responsible for the loss, damage or theft of any personal mobile device

- The sending of inappropriate text messages between any member of the school community is not allowed

- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Servers

- Newly installed servers holding personal data should be encrypted, therefore password protecting data.

- Always keep servers in a locked and secure environment

- Limit access rights to ensure the integrity of the standard build

- Always password protect and lock the server

- Existing servers should have security software installed appropriate to the machine's specification

- Back up tapes should be encrypted by appropriate software

- Data must be backed up regularly

- Back up tapes/discs must be securely stored in a fireproof container

- Back up media stored off-site must be secure

- Remote back ups should be automatically securely encrypted.

- Regular updates of anti-virus and anti-spyware should be applied

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

- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information

- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access

- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time

- Do not introduce or propagate viruses

- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or ECC 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).

Writing and Reviewing this policy.

- Members of staff have been involved in making/ reviewing the Policy for ICT Acceptable Use through an E-safety update as a staff meeting.

Review Procedure

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

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

This policy will be reviewed every (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 on…………………………….

-