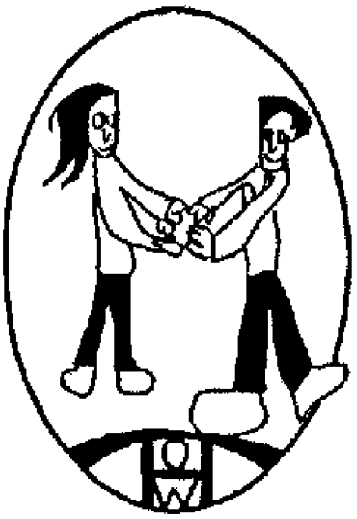
Howbridge Infant School



E-Safety and Data Security Policy

May 2025

Scope

This policy applies to all members of the school community (including staff, pupils, volunteers, parents, carers and visitors) who have access to, and are users of, school computing systems.

The school will manage e-safety as described within this policy. This will be in line with a number of policies in operation within the school including relationships and behaviour, anti-bullying, PSHE, safeguarding and child protection.

The e-safety policy will be reviewed by the Deputy Head and computing team and the Governing Body annually.

The school has a responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

The school holds personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties in line with the General Data Protection Regulations.

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, 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).

Roles and Responsibilities

The Headteacher is responsible for ensuring the safety of all members of the school community but the day to day responsibility for e-safety is delegated.

Role	Responsibility
Governors	● Approve and review the effectiveness of the e-safety policy ● Delegate a governor to be the Computing and Internet Safety link
SLT	● Create a culture where staff and learners feel able to report incidents ● Ensure that there is a system in place for monitoring e-safety ● Follow the correct procedure in the event of a serious e-safety allegation being made against a member of staff or a pupil ● Inform the local authority about any serious issues ● Ensure that the school infrastructure/network is as safe and secure as possible ● Ensure that policies and procedures around e-safety are implemented and followed ● Lead the e-safety committee ● Co-ordinate work with the school's designated safeguarding lead ● Provide training and advice for members of the school community ● Monitor, log and manage e-safety incidents
Computing/ e-safety co-ordinator	● Attend updates and ensure that CEOP training is up-to-date ● Manage the e-safety section of the school website ● Support the SLT in managing e-safety incidents ● Ensure all staff are aware of the e-safety policy and that all staff have signed the Acceptable Use Policy (AUP) ● Support the SLT in providing training and advice for members of the school community
Teaching and support staff	● Participate in any training and awareness raising sessions ● Read, understand and sign the staff AUP ● Act in accordance with the AUP and the e-safety policy ● Report any suspected misuse or problems to the SLT or e-safety co-ordinator
Pupils	● Agree class internet rules ● Participate in e-safety activities and report any suspected misuse
Parents	● Read the pupil AUP to their child and sign the agreement ● Discuss e-safety issues with their children and monitor home use ● Access the school website for e-safety information ● Keep up-to-date with issues through newsletters and other raising awareness opportunities ● Inform the Headteacher of any e-safety issues that relate to the school
Technical Support	● Ensure that the schools IT infrastructure is secure ● Ensure that all security updates are applied including anti-virus and Windows

Internet Filtering & Security

Filtering

The school has a managed filtering service in place with LGfL to block unwanted sites. The level of filtering can be adjusted to suit the level/age of each user, and is used in the e-safety of the pupils. The filtering service automatically blocks sites that are inappropriate based on a number of categories.

Firewall

A “firewall” is provided to protect against intrusions from the Internet, or indeed from other schools broadband users. In general the firewall works by excluding network traffic unless it has been explicitly permitted. The Schools broadband network has multiple firewalls that continue to provide the protection even if one should fail. The firewalls are monitored 24x7 for threats and intrusions to protect the schools broadband network.

Data Centre

The school's broadband network has a number of services provided from two high end data centres. These high security environments provide the location to host the core services for the Schools Broadband network. By combining these services in multiple locations the access to the services is maintained with little or no downtime to schools.

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 IT 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. Please see Appendices at the back of the policy detailing sanctions for misuse.

All breaches are logged in the B1 reporting template under GDPR.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the school's Senior Information Risk Owner (SIRO) or e-safety Co-ordinator. 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 IT and all other policy non-compliance must be reported to the SIRO.

The SIRO is the Headteacher.

Acceptable Use
Pupil Agreement

E-Safety Rules

- I will only use IT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my IT passwords.
- I will only open/delete my own files.
- I will make sure that all IT 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 unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe.
- I know that my use of IT can be checked and that my parent/carer contacted if a member of school staff is concerned about my E-Safety.

Agreement

We have discussed these rules …….....(child name) agrees

to follow the E-Safety rules and to support the safe use of IT at Howbridge Infant School.

Parent/ Carer Signature ……..……..…….

Class …….. Date ……

Acceptable Use
Staff Agreement

IT (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 IT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Ms A Conley, Howbridge Infant School, Senior Information Risk Owner.

- You **MUST** use our facilities economically; your personal use must not create extra costs for us.
- You **MUST NOT** use our facilities to undertake any unlawful, libellous, immoral or offensive activities, including accessing, downloading, storing, creating, copying or disseminating offensive material. This includes, but is not limited to, pornographic, sexual, violent or criminal content and racist, sexist or otherwise discriminatory material.
- You **MUST NOT**: Personal use must not interfere with your productivity and how you carry out your duties.
- You **MUST NOT**: Personal use must not reflect adversely on our reputation.
- You **MUST NOT**: You must not leave personal-use websites open during your working time, even if they are minimised on your screen and you are not actively viewing/ using them.
- You **MUST NOT**: You must not use browsers or access/ attempt to access sites that are knowingly unacceptable, even if this is in your own time.
- You **MUST NOT**: You must not send or forward chain, joke or spam emails.
- You **MUST NOT**: You must not use the Organisation's facilities for commercial purposes not approved by us or for personal financial gain.
- You **MUST NOT**: You must not use your access rights or identity as an employee to mislead another person, for personal gain or in any other way which is inconsistent with your role.
- You **MUST NOT**: You must not disclose (in writing, speech or electronically) information held by us unless you are authorised to do so, and the recipients are authorised to receive it.
- You **MUST NOT**: When you print, photocopy, scan or fax official-sensitive information, you must not leave the information unattended.
- You **MUST NOT**: You must not connect any equipment to our IT network that has not been approved.
- You **MUST NOT**: You must not do anything that would compromise the security of the information held by us, such as downloading/ spreading any harmful virus/ program or disabling or changing standard security settings.
- You **MUST NOT**: You must not make personal use of the information available to you that is not available to the public.
- You **MUST**: 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.
- You **MUST**: Comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- You **MUST**: Ensure that all electronic communications with pupils and staff are compatible with my professional role.
- You **MUST NOT**: Give out my own personal details, such as mobile phone number, personal e-mail address and social networking identities to pupils.
- You **MUST**: Only use the approved, secure e-mail system(s) for any school business.
- You **MUST**: 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 data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be stored on a password protected memory stick.
- You **MUST NOT**: Install any hardware of software without permission of the Senior Information Risk Owner (SIRO).
- You **MUST NOT**: Browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- You **MUST**: Ensure that images of pupils and/ or staff will only be taken, stored and used for professional purposes inline 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.
- You **MUST**: 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.
- You **MUST**: Respect copyright and intellectual property rights.
- You **MUST**: Ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- You **MUST**: Support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of IT and related technologies.
- You **MUST**: Understand this forms part of the terms and conditions set out in my contract of employment.

This Acceptable Use Agreement is a summary of our E-Safety Policy which is available in full via our school website.

User Signature

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

Signature

Date

Full Name (printed)

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. CD or memory stick) 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 IT equipment that you use.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates.
- If you suspect there may be a virus on any school IT equipment, stop using the equipment and contact your IT support provider immediately and the SIRO. The IT support provider will advise you what actions to take and be responsible for advising others that need to know.

Data Security and Data Protection

- The School gives relevant staff access to its Management Information System, with a unique ID and password.
- It is the responsibility of everyone to keep passwords secure.
- Staff are aware of their responsibility when accessing school data.
- Staff have been issued with the relevant guidance documents and the Policy for IT Acceptable Use.
- Leadership have identified Senior Information Risk Owner (SIRO) and Asset Information Owner(s) (AIO).
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data.
- Staff should avoid leaving any portable or mobile IT 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 IT 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.
- Anyone expecting a confidential/sensitive fax, should have warned the sender to notify the school before it is sent using the Safe Haven Fax procedure

---

Protective Marking

- All paper child protection data and documents are secured in a locked cabinet with restricted access.
- Any child protection concerns are recorded with a secure online system - CPOMs or written/printed on pink paper and then uploaded.
- All staff data and documents are secured in a locked cabinet with restricted access.
- All MIS databases have restricted password protected access.
- Any information passed between staff or governors that are confidential is labelled accordingly and sealed in an envelope and labelled as confidential.
- All emails containing sensitive information are marked OFFICIAL SENSITIVE STRICTLY CONFIDENTIAL.
- All confidential governor minutes are marked CONFIDENTIAL and printed on pink paper and are not available for public viewing.

Senior Information Risk Owner (SIRO)

The SIRO is the Headteacher.

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. Schools should identify an Information Asset Owner (IAO)

The role of an IAO is to understand:

- What information is held, and for what purposes
- What information needs to be protected (e.g. any data that can be linked to an individual, pupil or staff etc including UPN, teacher DCSF number etc)
- How information will be amended or added to over time
- Who has access to the data and why
- How information is retained and disposed of

The IAO for Howbridge Infant School is the Headteacher. As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

Although these roles have been explicitly identified, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Information Commissioner website

https://ico.org.uk/

General Data Protection Regulations – data protection guide, including the 8 principles

https://ico.org.uk/for-organisations/guide-to-data-protection/about-the-guide-to-data-protection/

Disposal of Redundant IT Equipment Policy

- All redundant IT equipment will be disposed of through an authorised agency only. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data
- All redundant IT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed.
- The school maintains an inventory of all its IT equipment including a record of disposal.

e-Mail

The use of e-mail within schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private unless they are marked as STRICTLY CONFIDENTIAL in-line with the protective marking guidance in this policy.

The school has implemented an email policy that automatically archives all emails after one year. After 3 years emails are deleted. The standard protection policy under the preset security policies on Microsoft Outlook and Google have been activated to provide greater security against spam, phishing and junk email.

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.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- The school requires a standard disclaimer to be attached to all e-mail correspondence.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- E-mails created or received as part of your role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account as follows:
  - ➢ Delete all 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 use appropriate language and not reveal 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 IT Subject Co-ordinator and the SIRO if they receive an offensive e-mail.
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending, reading or receiving business related e-mail is discouraged. However, it is recognised that in emergency situations this may be the only e-mail option available to staff.
- An outgoing e-mail greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming e-mail.
- School e-mail is not to be used for personal advertising.
- Check your e-mail regularly.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.

e-mailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using e-mail.
- 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 send the information to anybody/person whose details you have been unable to separately verify (usually by phone).
- Password protect confidential attachments and send the password in a separate email.
- Request confirmation of safe receipt.
  Wherever possible use secure email transfer software such as Egress that can encrypt your message and only decrypts the message once received by the recipient.

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

e-Safety

e-Safety - Roles and Responsibilities

As e-Safety 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. It is the role of the eSafety co-ordinator 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 e-Safety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

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

e-Safety in the Curriculum

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

- The school provides opportunities within a range of curriculum areas to teach about e-Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are taught about respecting other people's information, images, etc through discussion 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.

e-Safety Skills Development for Staff

- Our staff receive regular information and training on e-Safety issues in the form of staff meetings, email updates and where required training sessions.
- New staff receive information on the school's acceptable use policy as part of their induction and have a employee briefing paper regarding general data protection.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Managing the School e-Safety Messages

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used.
- E-Safety posters will be prominently displayed.

Incident Reporting, e-Safety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the school's SIRO. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of IT and all other policy non-compliance must be reported to the SIRO.

e-Safety Incident Log

Some incidents may need to be recorded in other places, if they relate to a bullying or racist incident.

HOWBRIDGE INFANT SCHOOL
e-Safety Incident Log

Details of ALL e-Safety incidents should be recorded. This incident log will be monitored termly by the Deputy Head.

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

Misuse and Infringements

Complaints

Complaints and/ or issues relating to e-Safety should be made to the e-Safety co-ordinator or the SIRO. Incidents should be logged.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the SIRO.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator, 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 by the SIRO.

Internet Access

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.

Managing the Internet

- Students 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.
- Google Safe Search should be used at all times.
- 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 what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- School internet access is controlled through the LGfL's web filtering service.
- Howbridge Infant 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.
- If staff or pupils discover an unsuitable site, the screen must be covered/turned off 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 IT Co-ordinator, 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 managers to install or maintain virus protection on personal systems.
- Staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Headteacher/IT Co-ordinator
- If there are any issues related to viruses or anti-virus software, the IT Co-ordinator should be informed.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting e-Safety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss e-Safety with parents/ carers and seek to promote a wide understanding of the benefits related to IT 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 containing the following statement or similar

We will support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community

- The school disseminates information to parents relating to e-Safety where appropriate in the form of;
    - Information and celebration evenings
    - Posters
    - Website/ Learning Platform postings
    - Newsletter items
    - Learning platform training

Cyberbullying

Cyberbullying along with all other forms of bullying of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

- The school will follow procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- The school will follow procedures to investigate incidents or allegations of cyberbullying.
- Pupils, staff, parents and carers are advised to keep a record of the bullying as evidence.
- The school will take steps where possible to identify the bully. This may include examining school system logs, identifying possible witnesses and contacting the service provider and the police.
- Pupils, staff, parents and carers will be required to work with the school to support the approach to cyberbullying and the schools e-safety ethos.
- Sanctions for those involved in cyberbullying will follow those for other bullying incidents and may include:
    - The perpetrator will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - Internet access may be suspended at the school for a period of time
    - Parents/carers of the pupils will be informed.
    - The police will be contacted if a criminal offence is suspected.

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 IT 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.
- Ideally, passwords should be a minimum of twelve characters and a mixture of upper and lower case letters, and numbers. You should try to use three random words
- User ID and passwords for staff and pupils who have left the School are removed from the system within 1 month.

If you think your password may have been compromised or someone else has become aware of your password report this to the e-Safety 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 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.
- Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer).

Zombie Accounts

Zombie accounts refer 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 staff has left the school.
- Prompt action on disabling accounts will prevent unauthorised access.

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure.
- 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 copy, scan or print.
- Only download personal data from systems if expressly authorised to do so by your manager.
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling.

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Ensure removable media is purchased with password protection.
- Store all removable media securely.
- Securely dispose of removable media that may hold personal data.
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.

Remote Access

- You are responsible for all activity via your remote access facility.
- Only use equipment with an appropriate level of security for remote access.
- To prevent unauthorised access to school systems, keep all information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone.
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment.

Taking of Images and Film

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

- Parental permission must be sought concerning the use of images.
- 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.
- Staff must follow the Safe use of Photographs Policy.

Publishing Pupil's Images and Work

All parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school website
- 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 the 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. Wherever possible we will contact parents before such images are used/published.

Parents/ carers may withdraw permission, in writing, at any time.

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

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

Storage of Images

- Images/ films of children are stored on the school's network and in secure cloud based servers based in the UK. Images are also stored on local devices such as ipads and laptops.
- Pupils and staff are not permitted to use personal portable media for storage of images without the express permission of the Headteacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform.
- The IT Technician has the responsibility of deleting the images at the end of each academic year,

on all pupil devices. Teachers are responsible for clearing all images and videos from their own laptops.

Webcams and CCTV

- The school uses CCTV for security and safety. The only person with access to this is the School Business 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.
- Misuse of the webcam by any member of the school community will result in sanctions.

    - Webcams can be found on teacher's laptops and on all ipads. Staff must inform the audience that the webcam is in operation.

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

School IT Equipment

- As a user of IT, you are responsible for any activity undertaken on the school's IT equipment provided to you.
- All IT equipment issued to staff is logged and serial numbers are recorded as part of the school's inventory.
- Do not allow your visitors to plug their IT hardware into the school network points (unless special provision has been made). They should be directed to the wireless IT Facilities if available.
- Ensure that all IT 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 or on google drive.
- Personal or sensitive data should not be stored on the local drives of laptops or PCs. In particular no pupil data should be stored on local drives.
- It is recommended that a time locking screensaver is applied to all machines. Any IT equipment accessing personal data must have a locking screensaver.
- Privately owned IT equipment should not be used on a school network.
- On termination of employment, resignation or transfer, return all IT 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 IT 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 teams
    - recovering and returning equipment when no longer needed

- All redundant IT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA).

Portable & Mobile IT Equipment

This section covers such items as laptops, PDAs 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's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be password protected.
- 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.
- Ensure portable and mobile ITT 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 IT Co-ordinator, fully licensed and only carried out by our IT support.
- In areas where there are likely to be members of the general public, portable or mobile IT equipment must not be left unattended and, wherever possible, must be kept out of sight.

Mobile Technologies

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use but these must not be used during lesson time. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.
- Pupils are NOT allowed to bring personal mobile devices/phones to school.
- 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.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Staff are able to use their mobile phone devices to support 2FA on their email and google drive accounts.

Servers

- Limit access rights to ensure integrity.
- Always password protect and lock the server.
- Data must be backed up regularly.
- Remote backups 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.
- Do not allow any unauthorised person to use school IT 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 log off from the equipment 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 IT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school 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).
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act.
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in a way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing of the data.

METHODS OF COMMUNICATION

	Staff & Other Adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons (unless for authentication purposes)				✓				✓
Use of mobile phones in break times	✓							✓
Taking photos on school owned mobile phones or other camera devices for educational purposes	✓							✓
Use of handheld devices, such as PDAs		✓						✓
Use of personal email addresses in school, or on school network			✓					✓
Use of school email for personal emails			✓					✓
Use of chat rooms			✓					✓
Use of instant messaging			✓					✓
Use of social networking sites			✓					✓
Use of blogs			✓					✓
Use of twitter			✓					✓
Use of you tube			✓					✓

USE OF THE INTERNET

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable
On-line games (educational)		✓		
On-line games (non-educational)				✓
On-line gambling				✓
On-line shopping			✓	
File sharing			✓	

SANCTIONS FOR MISUSE: PUPILS

	Refer to Class Teacher	Refer to Head	Refer to Police	Refer to technical support staff for action (filtering/ security)	Inform parents /carers	Removal of network / internet access rights	Warning	Further sanction exclusion
Deliberately accessing or trying to access material that could be considered illegal	✓	✓	✓		✓	✓		✓
Unauthorised use of non-educational sites during lessons	✓	✓			✓		✓	
Unauthorised use of mobile phones/digital cameras/other hand held devices	✓	✓			✓		✓	
Unauthorised use of social networking/instant messaging/personal email	✓	✓			✓		✓	
Unauthorised downloading or uploading of files	✓	✓			✓		✓	
Allowing others to access school network by sharing usernames and passwords	✓	✓			✓		✓	
Attempting to access or accessing the school network using another pupils account details	✓	✓			✓		✓	
Attempting to access or accessing the school network using the account of a member of staff	✓	✓			✓		✓	
Corrupting or destroying the data of others users	✓	✓			✓		✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓			✓		✓	
Continued infringements of the above following previous warnings or sanctions	✓	✓			✓		✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓			✓		✓	
Using proxy sites or other means to subvert the school's filtering system	✓	✓		✓	✓	✓		
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓		✓	✓			
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓	✓	✓	✓	✓
Receipt or transmission or material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓			✓		✓	

SANCTIONS FOR MISUSE: STAFF

	Refer to HT	Refer to LA/HR	Refer to LAO (L)/ Police(P)	Refer to Technical Support Staff	Warning	Suspension	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal	✓	✓	L,P		✓	✓	✓
Excessive or inappropriate personal use of internet/social networking/instant messaging/personal email	✓				✓		
Unauthorised downloading or uploading of files	✓				✓		
Allowing others to access the school network by sharing username and passwords, or attempting to access or accessing the school network, using another person's account	✓				✓		
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓				✓		
Deliberate action to breach data protection or network security rules	✓	✓			✓		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓		P				✓
Sending an email, text or instant message that is offensive, harassment or of a bullying nature to staff	✓	✓			✓		
Sending an email, text or instant message that is offensive, harassment or of a bullying nature to learners	✓	✓	L		✓	✓	✓
Breach of the school e-safety policies in relation to communication with learners	✓		L		✓		
Using personal email/social networking/instant messaging/text messaging to communicate with pupils	✓		L		✓		
Actions which could compromise staff members standing	✓				✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓				✓		
Using proxy sites or other means to subvert the schools filtering system	✓				✓		
Accidentally accessing offensive or pornographic material and failing to report the incident	✓		L		✓		
Deliberately accessing or trying to access offensive or pornographic material	✓		L				✓
Breaching copyright or licensing regulations	✓				✓		
Continued infringements of the above, following previous warnings or sanctions	✓		P				✓