ICT Acceptable Use Incorporating ESafety, Data Security & Disposal of ICT Equipment

September 2023

At Gravenhurst Academy 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.

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, Net books, whiteboards, digital equipment etc) and technologies owned by pupils and staff, but brought onto school premises (such as mobile phones and portable media players etc)

Monitoring

All internet activity is logged by the school's internet provider. These logs may be monitored by authorised local authority staff.

Breaches

A breach or suspected breach of policy by a School employee or contractor 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

Incident Reporting

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

Computer Viruses

All files downloaded from the internet, received via e-mail or on removable media (e.g. USB pens, 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 is.

If the machine is not routinely connected to the school network, you must make provision for regular virus updates.

If it is suspected that there may be a virus on the school ICT equipment you must stop using the equipment and inform eSafety Coordinator or School Business Manager.
Security (see IT security policy)

E – Safety Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Head Teacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is Miss Rowlands

All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through Central Bedfordshire LA.

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

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

Senior Information Risk Owner (SIRO)

- The SIRO owns the information risk policy and risk assessment
- Keeps a record of all Information Asset Owners (IAOs)
- Act as an advocate for Information risk management.

The SIRO in this school is Mrs Meller

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff, medical information and special educational needs data.

The IAO in this school is Mrs Meller

The role of the 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 a 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.

Although these roles have been explicitly identified, the handling of secured data is everyone's responsibility. Failing to apply appropriate controls to secure data could amount to gross misconduct.

Disposal of Redundant ICT Equipment Policy

- 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
Data Protection Act 1998
Electricity at Work Regulations 1989

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.
- The school's disposal record will include: Date item disposed of Authorisation for disposal, including
- Verification of software licensing
- Any personal data likely to be held on the storage media
- How it was disposed of e.g. waste, gift, sale
- Name of person and/or organisation who received the disposal item.

Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

e-Mail

- The school gives all staff their own e-mail account, through the learning platform, 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.
- The school requires a standard disclaimer to be attached to all e-mail correspondence stating that the views expressed are not necessarily those of the school or LA. The responsibility for adding this disclaimer lies with the account holder.

- 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 is advised to cc the Head teacher, 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 Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follow;
- Delete all e-mails or short-term value
- Organise email into folders and carry out frequent house-keeping on all folders and archives.

- All pupils have their own individual account giving them access to the learning platform.
- The forwarding of chain letters is not permitted in school. However the school has set up a dummy account to allow pupils to forward any chain letters causing them anxiety. No action will be taken with this account by any member of the school community.
- All pupil e-mail users are expected to adhere to the generally accepted rules of net-iquette 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 email.
- Staff must inform the eSafety co-ordinator 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, all the school e-mail policies apply.
- The use of Hotmail, BT Internet, AOL or any other internet-based web mail service for sending, reading or receiving school business related e-mail is not permitted.

Sending e-mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the section e-mailing Personal, Sensitive, Confidential or Classified Information.
- Use your own school e-mail account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.
- School e-mail is not to be used for personal advertising.

Receiving e-mails

- Check your e-mail regularly
- Never open attachments from an untrusted source. Consult the 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.
- The automatic forwarding and deletion of e-mails is not allowed.

e-mailing Personal, Sensitive, Confidential 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 where possible.
- The use of Hotmail, BT Internet, AOL or any other Internet based web mail 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:
    - Obtain express consent from your manager to provide the information by e-mail.
    - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:-
        - Verify the details, including accurate e-mail address, of any intended recipient of the information.
        - Verify (by phoning) the details of a requestor before responding to e-mail requests for information.
        - Do not copy or forward the e-mail to any more recipients than is absolutely necessary.

      Do not send the information to any body/person whose details you have unable to separately verify (usually by phone)

      Send the information as an encrypted document **attached t**o an e-mail.

      Provide the encryption key or password by a separate contact with the recipient(s)

      Do not identify such information in the subject line of any e-mail

      Request confirmation of safe receipt.

Equal Opportunities

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

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanations to reinforce their existing knowledge and understanding eSafety issues. – Teaching of the CEOPS is taught throughout the school.

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

eSafety in the Curriculum

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

- The school teaches internet skills in ICT/PSHE lessons. (see ICT and PSHE scheme of work)
- 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 taught about respecting other people's information images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. |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 Child line/CEOP report abuse button.

eSafety Skills Development for Staff

- Our staff receives regular information and training on eSafety issues in the form of termly staff meetings.
- Details of the ongoing staff training needs can be found in the CPD coordinators file.
- New staff receives 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 knows 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 eSafety Messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.
- The eSafety policy will be introduced to the pupils at the start of each school year.
- ESafety posters will be prominently displayed.

Incident Reporting, eSafety Incident Log & Infringements

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

eSafety Incident Log
Some incidents may need to recorded in other places, such as the Behaviour Log, if they relate to a bullying or racist incident. – see appendix A

Misuse and Infringements
Complaints relating to eSafety should be made to the eSafety coordinator or Head teacher.

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 coordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety coordinator, depending on the seriousness of the offence, investigation by the Head teacher, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

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 invaluable resources for education, business and social interaction as well as a potential risk to young and vulnerable people.

Managing the Internet

- The school maintains student account that 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 however under supervision pupils will use google.co.uk
- 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 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 Head teacher'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.
- Our school also employs some additional web filtering which is the responsibility of Courtlands Service Providers.
- Gravenhurst Lower is aware of its responsibility when monitoring staff communication under current legislation and takes into account, Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.
- It is the responsibility of the school, by delegation to the network manager to ensure that anti-virus protection is installed and kept up to date on all school machines.
- Pupils and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the Head teacher.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed through the school office.

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

- At present, the school endeavours to deny access to social networking 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, email address, specific hobbies/interests)
  Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incident of bullying to the school.
- Staff may only create blogs, or web spaces in order to communicate with pupils using the LA Learning Platform or other systems approved by the Head teacher.

Parental Involvement
We believe that it is essential for parents/carers to be fully involved with promoting esafety both in and outside of school. We regularly consult and discuss e-safety 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)

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

- Information and celebration evenings
- Posters
- Website/Learning Platform postings
- Newsletter items
- Learning Platform training.

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.

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 and 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. From Year 3 they are also expected to use a personal password and keep it private.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS system and/or Learning Platforms, including ensuring that passwords are not shared and are changed periodically.
- Due consideration should be given when logging into the Learning Platform to the browser 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 account when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left.
- Prompt action on disabling accounts will prevent unauthorised access.
- Regularly change generic passwords to avoid unauthorised access (Microsoft© advise every 42 days)

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and classified Information

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

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

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

- Ensure removable media is purchased with encryption Store all removable media security.
- Securely dispose of removable media that may hold personal data.
- Encrypt all files containing personal, sensitive, confidential or classified data.
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.

School ICT Equipment including Portable & Mobile ICT Equipment and 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.
- ICT equipment issued to staff will have serial numbers recorded as part of the school's inventory.
- All ICT equipment will be kept physically secure.
- Privately owned ICT equipment should not be used on the school network.
- On termination of employment, resignation or transfer, all ICT equipment must be returned. Logons should be disabled.
- All redundant ICT equipment will be disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

This section covers such items as laptops, net books, and removable data storage devices.

- All activities carried out on the 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 care before starting your journey.
- 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 team.
- Portable equipment must be transported in its protective case if supplied.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones 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.
- 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.
- Under no circumstances should staff use their own mobile device for taking pictorial images of pupils.
- Users bringing personal devices into school must ensure there is not inappropriate or illegal content on the device.

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed.
- Where the school provides mobile technologies such as phones and laptops for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, this device may only be used to conduct school business outside of school, and not for social use.

Removable Media

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

- Only use recommended removable media
- Store all removable media securely
- Removable media must be disposed of securely by the ICT support team

Servers

- The server has limited access rights
- The server is password protected and the server console is locked. Data is backed up weekly
- Backed up data is stored off-site.

Writing and Reviewing this Policy

- Staff and pupils have been involved in reviewing the Policy for ICT Acceptable Use through staff meetings and school council meetings.

- 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 annually 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 ……Ann Gilbert……. On behalf of the Governing body.

Head Teacher -Debbie Randall Date October 2023

Chair of Governors -Ann Gilbert Date November 2023

Review Date- November 2024