Education Partnership Trust

Creating outstanding schools which transform learning, lives and communities

ICT SECURITY POLICY

Document Control

This document has been approved for operation within:	All Trust Establishments
Date effective from	December 2022
Date of next review	December 2023
Review period	Annual

Contents

1. INTRODUCTION

1.1 This policy outlines the secure and safe use of computer equipment.

1.2 The Education Partnership Trust is committed to protecting employees, partners and students from illegal or damaging actions by individuals, either knowingly or unknowingly. The School and Trust will take appropriate steps to protect ICT equipment, resources and environments from threats, including but not limited to unauthorised access, computer viruses, violation of privacy and interruption to service.

2. PURPOSE

2.1 The purpose of this policy is to:

- Define the acceptable use of school/Trust ICT resources and equipment.
- Ensure all use of the ICT resources and equipment is legal, ethical, and consistent with the aims, values and objectives of our school/Trust.
- Inform all users of their personal responsibilities when using the school/Trust ICT resources and equipment and environment.
- To protect our school's/Trust's IT environment from all threats whether internal or external.
- To ensure that those who use school/Trust ICT resources, equipment and networks are aware of the requirements of IT Security and Acceptable Use.
- To ensure that users are aware of their roles and responsibilities in applying, enforcing and complying with ICT Security and Acceptable Use.

3 OBJECTIVES

3.1 The objectives of this policy are:

- to ensure that equipment, data and staff are adequately protected on a cost-effective basis against any action that could adversely affect the school/Trust;
- to ensure that staff users are aware of and fully comply with all relevant legislation and guidance around ICT security and safe and acceptable use of ICT;
- to create and maintain within the school/Trust a level of awareness of the need for ICT security to be an integral part of the day to day operation so that all staff understand the need for ICT security and their own responsibilities in this respect.

4 DEFINITIONS

4.1 For the purposes of this document the terms 'ICT' (or 'ICT system') 'ICT environment, 'ICT data' and 'ICT user' are defined as follows:

- 'ICT' (or 'ICT system') means any device for automatic storing and processing of data and includes mainframe computer, minicomputer, microcomputer, personal computer (whether handheld laptop, portable, stand-alone, network or attached to a mainframe computer), workstation, word-processing system, desk top publishing system, office automation system, messaging system, any other similar device and peripherals for these devices.

- ICT environment means any virtual, online, networked or computer-based resource or facility available through the school.
- 'ICT data' means any information stored and processed by ICT and includes programs, text, pictures and sound; see appendices 4 and 5
- 'ICT user' applies to any employee, member of school staff, pupil or other authorised person who uses the school's ICT systems and/or data.

5 SCOPE

5.1 This policy applies to all users of school ICT environment and equipment and must be adhered to at all times. It also sets expectations for the appropriate, legal and safe use of all equipment in school, including devices belonging to staff and pupils. It also covers:

- All equipment that is owned or leased by school.
- Guest devices authorised by school.
- All employees, contractors and temporary staff, outsource agents and other workers at school who are responsible for the administration and management of the school ICT equipment and resources.
- All those who use the school ICT services including both students and staff.
- When reviewing this document in regard to the concerning the Trust central office, the term 'school' is interchangeable with 'Trust'

6 EXPECTATIONS

6.1 The appropriate Acceptable Usage Agreement should be signed by all staff and pupils, and a parent or guardian of each pupil. A signed AUA form should be returned before a user is permitted access to ICT equipment and services. Signed AUPs are stored safely in the School Office**.** All school staff have a responsibility to familiarise themselves with the relevant sections of this policy before using the school ICT equipment and environment. Each staff user must read, understand and sign to verify they have read and accepted this policy before using the ICT equipment and environment (Appendix 1).

6.2 Any user found to have breached the terms of this policy, may be subject to the Trust disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

7 COMPLIANCE WITH POLICY

7.1 The ICT environment is provided to support learning within the education system. All those accessing the school ICT environment will comply with all current legislation in England, in addition to any requirements placed on them by this security policy. This includes compliance with legislation designed to protect personal information, legislation covering software and similar intellectual property licensed from third parties, and cooperation with Law Enforcement agencies. If in any doubt, the user should seek advice from the Headteacher.

COMPLIANCE WITH POLICY FOR ALL USERS

7.2 The primary usage will be to support school educational and pastoral activities. Full compliance with the acceptable use policies and policy standards is expected, including:

- Compliance with and adoption of the agreed password standards (Appendix 2)
- Adoption of safe practices to ensure the integrity of the ICT environment, password security and data security.
- Compliance with the appropriate reporting mechanisms should they suspect an account has been compromised, ICT security breached, or a safeguarding issue arise. In the first instance, for SIMs this would be the School Business Manager and the ICT Technician for other breaches. They would then ensure that this is reported to the Headteacher.

7.3 The ICT resources and equipment are provided primarily for the purpose of conducting and supporting learning and teaching activities; however personal usage of school, LA or personal equipment is permitted as long as that does not:

- Take place during lesson time or otherwise interfere with the user's professional role.
- Bring the school or Trust into disrepute.

7.4 All users should be aware that usage may be monitored and/or recorded; misuse of the ICT equipment and environment may lead to disciplinary action. In such situations, the Headteacher and EPT will be the arbiters of whether or not the use was reasonable in the circumstances.

COMPLIANCE WITH POLICY FOR ALL SCHOOL STAFF

7.5 In general, the acceptable use standard for school staff is the same as for students except:

- It is acceptable for a member of the school staff to access and use one of their pupils' accounts, in order to assist the pupil in using the ICT resources and equipment.
- It is acceptable for a member of the school staff to access a student's files.
- Members of the school staff should not use any other users ICT Service user account login for work or personal matters.
- Whilst legally school staff have a right to delete files considered to be inappropriate that are on a pupil's personal device, members of staff should not delete content of files from devices. Correct procedure is to report this to the E-Safety Lead.
  Searching, screening and confiscation at school - GOV.UK (www.gov.uk)

COMPLIANCE WITH POLICY FOR TEMPORARY USERS

7.6 All temporary users will be required to:

- Sign the acceptable use agreement and agree to abide by the requirements set out in this policy.
- Sign the relevant E-Safety AUA and agree to abide by the E-Safety policy.

COMPLIANCE WITH POLICY FOR OPERATIONS STAFF

7.7 Technical support staff may have access to other users' information and files within the ICT environment. This information will only be accessed for operational purposes. It must never be copied outside the ICT environment. Inappropriate access to, or misuse of, personal information within the ICT environment will be considered a disciplinary offence.

8 ICT SECURITY

8.1 A number of different groups have responsibility within school ICT for aspects of ICT Security.

GOVERNING BODY RESPONSIBILITIES

8.2 The governing body has ultimate corporate responsibility for ensuring that the school complies with the legislative requirements relating to the use of ICT systems and for disseminating policy on ICT security and other ICT related matters. In practice, the day-to-day responsibility for implementing these legislative requirements rests with the Headteacher.

HEADTEACHER RESPONSIBILITIES

8.3 The Headteacher is responsible for ensuring that the legislative requirements relating to the use of ICT systems are met and that the school's AUP/ICT Security Policy is adopted and maintained by the school. He/she is also responsible for ensuring that any special ICT security measures relating to the school's ICT facilities are applied and documented as an integral part of the Policy.

8.4 The Headteacher, in accordance with the School's Financial Regulations, shall ensure that an inventory of all ICT equipment (however financed) is maintained, and all items accounted for at least annually.

8.5 In practice, the day to day functions may be delegated to a named member of school or technical staff, who will keep an inventory of equipment **within** their remit.

8.6 The Headteacher is also responsible for ensuring that the requirements of the General Data Protection Regulation and the Data protection Act 2018 (Appendix 5) are complied with fully by the school. This is represented by an on-going responsibility for ensuring that the:

- Registrations under the GDPR and DPA are up-to-date and cover all uses being made of personal data.
- Registrations are observed with the school.
- School has a current Data Protection Policy, clearly defining how they assess and record levels of protection data.

8.7 In addition, the Headteacher is responsible for ensuring that users of systems and data are familiar with the relevant aspects of the Policy that the appropriate controls are in place for staff to comply with the Policy. The Headteacher or Chair of Governors should ensure that details of any suspected or actual breach are recorded and made available to Internal Audit upon request. The Headteacher or Chair of Governors must advise Internal Audit of any suspected or actual breach of ICT security pertaining to financial irregularity.

INTERNAL AUDIT RESPONSIBILITIES

8.8 The Internal Audit Section of the EPT is responsible for checking periodically that the measures prescribed in each school's approved ICT Security Policy/AUP are complied with, and for investigating any suspected or actual breaches of ICT security.

SCHOOL RESPONSIBILITIES

8.9 The Governing Body and Headteacher are ultimately responsible for all school responsibilities. The school is responsible for:

- Ensuring appropriate arrangements are applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.
- Giving adequate consideration to the physical security of rooms containing ICT equipment (including associated cabling). As far as practicable, only authorised persons should be allowed access to the school's server or servers that provide access to data.
- Defining and documenting the requisite level of protection for data and documents according to the information classification system.
- Defining and documenting appropriate levels of access to the network and associated resources including the Information Management System.
- Ensuring staff with higher levels of access sign any additional documentation as required.
- Ensuring the Ethical and safe disposal of decommissioned equipment.
- Ensuring the Integrity of data, both during repair of faulty equipment and the disposal of assets.

USER ACCOUNTS

8.10 Access to the environment will be by individual user account for staff, who will be required to comply with minimum password standards and pupils have a common password but are taught the importance of securing their documents (See Appendix 2 for guidance on standards for passwords).

- Enabled user accounts are available only for current staff and pupils.
- The user account of anyone who is under investigation for inappropriate use of the system must be disabled promptly.
- 'Generic' or group usernames (i.e. accounts that could be used by more than one person) will only be created in special circumstances and must be agreed beforehand by the Headteacher and access restricted as appropriate.

8.11 Access to another user's data may be given in exceptional circumstances. Should this be required users should seek advice from the Headteacher.

EQUIPMENT SITING

8.12 Reasonable care must be taken in the siting of computer screens, keyboards, printers or other similar devices. Whenever possible, and depending upon the sensitivity of the data, users should observe the following precautions:

- Devices should be positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information. Specific consideration should be given to the siting of devices on which confidential or sensitive information is processed or retrieved;
- Users should avoid leaving computers logged-on when unattended if unauthorised access to the data held can be gained. Clear written instructions to this effect should be given to users;
- A 'clear desk policy', i.e. hard copies of sensitive data are not left unattended on desks;

8.13 The same rules apply to school equipment in use at a user's home or when accessing sensitive data using home equipment.

ADULT USERS' RESPONSIBILITIES

8.14 All users will sign a user agreement at an appropriate level, before using the school's ICT equipment. All users of the school's ICT systems and data must comply with the requirements of this Acceptable Use Policy, which are summarised in *Acceptable Use Agreement*' attached as Appendix 1. Pupils will sign an appropriate acceptable use agreement and should be guided by school staff towards respecting and conforming to the expectations of this policy.

All users are responsible for:

- The use of their unique logon details (usernames and passwords), email address where provided and for all content that is transmitted received and stored by their user account. It is of utmost importance that the password and access to a user's account remains protected at all times (Appendix 2).
- Reporting concerns over password security immediately.
- Users are responsible for notifying the Headteacher of any suspected or actual breach of ICT security. Where the level of breach requires it, the Headteacher should inform Internal Audit.
- Looking after all computer equipment, ensuring they leave PCs and peripherals in the condition in which they were found.
- Ensuring any mobile devices used in school are, when not in use, switched off fully, connected for charging and stored in a secure place.
- Ensuring pupils in their care are reminded regularly of expectations around appropriate use of ICT equipment security and E-Safety.
- Returning portable equipment signed out to them for updates when requested to do so.
- Endeavouring to protect school equipment and the network against Viruses, Malware and other forms of software based attacks by virus checking portable devices and following only reliable, known links.
- Reporting any inappropriate use of ICT services (see section 7).
- Following the ICT Asset Protocol when taking any school equipment off the schools' premises.
- Users should report any incidents, either perceived or real, to the Headteacher at their school. The Headteacher is responsible for escalating such incidents to the technical support service, Internal Audit or other organisation as appropriate.
- All staff should ensure all personal data (pupil/parent/staff) held and used by them is either returned to school ownership or destroyed when leaving employment. Failure to do this may constitute a breach of data protection rules by school.

8.15 Users should not make any attempt to disable or reconfigure any ICT security measures or software, including Anti-virus software or seek to bypass any monitoring, filtering or security measures that are in place.

8.16 **Users are responsible for ensuring all data requiring backup is stored on the server and not saved on individual computers.**

STAFF USERS' ADDITIONAL RESPONSIBILITIES

8.17 Where users have access to sensitive data, they will receive training on data security before accessing data at an appropriate level on the managed service network. Staff users are responsible for:

- Protecting access to their account, and for maintaining the appropriate confidentiality of their data.
- Ensuring privacy of pupil data
- Storing data appropriately
- Ensuring pupils in their care are reminded regularly of expectations around appropriate use of ICT equipment security and E-Safety.
- Returning portable equipment signed out to them for updates when requested to do so.

SCHOOL TECHNICAL SUPPORT

8.18 At school we insist that all technical support staff fully understands and complies with the requirements of the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA) and all legislation around the control and storage of data. Technical Support have responsibility for:

- Ensuring all data held on the curriculum server is backed up and this process meets Government baseline security criteria.
- Bringing any security incidents, either perceived or actual, to the attention of the Headteacher.
- Management of the ICT network, ICT equipment, systems and data including controlling access to these assets under the instruction of The Headteacher.
- Integrity of data during both repairs of faulty and disposal of equipment.
- measures to guard against unauthorised access to data, such as ensuring that all data is held in a secure location.
- Ensuring approved security patches and service packs are in place on all devices.
- Administering the practical aspects of ICT protection and ensure that various functions are performed, such as maintaining the integrity of the data, producing the requisite back-up copies of data and protecting the physical access to systems and data.

9 DATA SECURITY

9.1 The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

PASSWORDS

9.2 All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

9.3 Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

9.4 Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

9.5 All staff and students will be allocated a password by the IT team. Staff must ensure that they update their password regularly and also keep student passwords, which are allocated, safe and secure.

SOFTWARE UPDATES, FIREWALL AND ANTI-VIRUS SOFTWARE

9.6 All of the school's ICT devices that support software updates, security updates and anti-virus products will be configured to perform such updates regularly or automatically.

9.7 Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

9.8 Any personal devices using the school's network must all be configured in this way.

DATA PROTECTION

9.9 All personal data must be processed and stored in line with data protection regulations and the school's data protection policy. EPT Data Protection Policy.

ACCESS TO FACILITIES AND MATERIALS

9.10 All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

9.11 These access rights are managed by the IT manager at the school and/or trust

9.12 Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the IT manager at the school and/or trust immediately.

9.13 Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

ENCRYPTION

9.14 The school ensures that its devices and systems have an appropriate level of encryption.

9.15 School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the Headteacher.

9.16 Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the IT manager.

10 PROTECTION FROM CYBER ATTACKS

10.1 Please see the glossary (Appendix 7) to help you understand cyber security terminology. The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - '**Proportionate'**: the school will verify this using a third-party audit (such as this one) annually, to objectively test that what it has in place is up to scratch
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up-to-date**: with a system in place to monitor when the school needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be
- Back up critical data minimum once a day and store these backups on [cloud-based backup systems/external hard drives that aren't connected to the school network and which can be stored off the school premises]
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to cloud based provider and/or IT provider
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department, for example, including how the school will communicate with everyone if communications go down, who

will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

11 ONLINE COMMUNICATION AND USE OF THE WEB TO DOWNLOAD/UPLOAD INFORMATION

PROVISION – INTERNET ACCESS

11.1 The provision of the Internet access is owned by school and all access is, recorded and logged. This supports the performance of internal investigations and the management of systems as well as helping to ensure compliance in accordance with the Regulation of Investigatory Powers Act 2000.

11.2 Users browse the Internet through a filtered service that is designed to reduce the risk of access to inappropriate material. Nevertheless, this filtering cannot be 100% effective, and users should be aware of the possibility of access to inappropriate material and know what to do if such material is displayed. Please note that this service is managed by school. Where a user's job role requires them to access sites that may be considered inappropriate approval must be obtained from their Headteacher prior to access.

11.3 Staff with access to the school's email should be aware that the content of emails and attachments may need to be disclosed under the GDPR and DPA (Appendix 5) and the Freedom of Information Act 2000. Email use is filtered and can be recorded.

GUIDANCE ON USE

11.4 All use of electronic forms of communication or use of the web to share, access download or publish information, should:

- Ensure that personal and financial information is safeguarded, including personal contact details.
- Ensure the security of the ICT network by maintaining up to date virus protection and following links downloading files from reliable sources only.
- Always use a school email address when sending, receiving or forwarding emails containing RESTRICTED information.
- Access news groups, bulleted boards and other similar communication groups for educational purposes or those relating specifically to their professional role only.
- Use social networking sites, real time chat, discussion forums, online games and other similar web resources only when expressly permitted to do so for educational purposes, or as part of a member of staff's professional role.
- Only publish information they have permission to use from the school and individuals
- Abide by copyright laws and licensing constraints regarding the use of software and electronic media.

11.5 Boundaries around publishing publicly accessible information and resources should be agreed on a school by school basis, with staff given appropriate permissions and clear guidelines as to acceptable content.

11.6 Use of electronic forms of communication or web access to share, download or publish information, for the following purposes is not permitted and may result in disciplinary and legal action where necessary.

- Sending, receiving, accessing or downloading obscene, racist, or insulting language, images, video or other media.
- Sending, receiving, accessing or downloading content in any form, containing provocative, suggestive or discriminatory language.
- Engaging in activities that bully, harass, mislead others or cause distress to groups or individuals.
- Accessing sites that are violent, hateful and discriminatory, promote hacking, or encourage gambling.
- Revealing information of a personal or private nature, or information that may lead to identification of an individual.
- Sending SPAM
- Downloading, uploading sharing or copying any content of copyrighted material, unless permission has been sought and given by the owner of the copyright (Please note breaching this is a criminal act and may lead to personal prosecution).
- Forwarding emails or information containing personal, confidential or sensitive information (therefore, classified as PROTECT or RESTRICTED information - see Information Classifications Section) from school email addresses to any personal email addresses including the employee's own personal email.
- Sending or forwarding emails containing RESTRICTED information to recipients outside the school who do not have school email accounts. This should be done through your standard school email address with appropriate encryption. Contact the IT.
- Using the school IT Systems to support private business or money-making activities.
- Any use that may potentially bring the users, the school and or the EPT into disrepute. (where a user is unsure whether a particular use is acceptable, it is their responsibility to consult the Headteacher).

12 PORTABLE DEVICES AND EXTERNAL CONNECTIONS

12.1 Facilities are in place to allow the transfer of information into and out of the school ICT environment by removable media (e.g. CD, pen drive, flash memory card, removable hard drive etc). Automatic anti-virus and security tools are in operation to scan material during such transfers.

EXTERNAL NETWORK CONNECTIONS

12.2 Requests for external connections to access the school's ICT Network, must be brought to the attention of school SLT, who will establish whether it is safe to permit such access.

REMOVABLE MEDIA AND MOBILE DEVICES

12.3 Securing PROTECTED or RESTRICTED data is of paramount importance – particularly in relation to school need to protect data in line with the requirements of the Data Protection Act1998. When using portable devices and removable media:

- Permission should be sought from the Headteacher and an assessment of risks, especially relating to information assurance, should be carried out before taking mobile devices out of the school site or using cloud technology to store work related information (Appendix 3).
- Users should sign to acknowledge receipt of loan devices.

12.4 Users should not engage in the following activities when using portable devices and removable media:

- Any action designed to circumvent anti-virus and ICT security measures when connecting school equipment to private networks, or when accessing school resources through private networks.
- Storage of PROTECT or RESTRICTED material (Appendix 4).
- Storing any data on removable media or mobile devices once it has been transferred/used.

DEVICES CONNECTED TO THE TRUST OR SCHOOL ICT NETWORK

12.5 Any device connected to school's ICT network must comply with the following rules:

- All network servers and desktops must have adequate, up-to-date anti-virus protection or endpoint security tools with automatic updates.
- Up-to-date security patches and service packs must be in place on all devices.
- Authority must be sought from the Headteacher before guest devices can be connected to the school network.

12.6 Any loss or theft of removable media or portable devices must be reported immediately to the Headteacher.

STORAGE AND INSTALLATION OF SOFTWARE, RESOURCES AND DATA

12.7 The use and storing of information by school is controlled by certain Acts of Parliament. There are obligations for the School and members of its community that must be followed (Appendix 5).

12.8 The owner has the legal title to the property. In this respect, all software, data and associated documentation produced in connection with the work of the school are the legal property of the EPT, which will normally hold it for the benefit of school.

12.9 Exceptions to this will be allowed for software and documentation produced by individual Teachers when agreed in writing by the Headteacher.

12.10 We also use software and data that are the legal property of external organisations and which are acquired and used under contract or licence.

LICENCES

12.11 Software license compliance requires all software used within the School is legally licensed, in accordance with the Copyright, Designs and Patents Act 1998.

12.12 It is the school's responsibility to ensure that all software on the ICT network is appropriately licensed.

12.13 The school is responsible for compiling and maintaining an inventory of all software held by the School and for checking it at least annually to ensure that software licences accord with installations.

12.14 To ensure the School is compliant the following rules must be adhered to:

- All software must be purchased with a licence appropriate to its intended use.
- The school expressly prohibits the illegal duplication of software.
- Copying, downloading and storing of copyrighted material (such as music, and photographs from magazines) that is not waivered for educational use is strictly prohibited.
- It is the school's responsibility to ensure that software added to all devices and desktops including guest devices, is appropriately licensed.

12.15 **Please be aware that failure to follow this policy could lead to criminal prosecution.**

13 DATA OWNERSHIP

13.1 Data within school ICT environment will be owned by a number of different individuals and organisations. The EPT will have the final decision on the ownership of any particular item. All data will be handled in a manner appropriate to its sensitivity.

LEGAL RESPONSIBILITY

13.2 The EPT and school collects, holds and uses data about people and organisations with whom it deals with in order to conduct its business.

13.3 The EPT and school fully endorses and adheres to the Principles of Data Protection as set out in the GDPR and the DPA, and other relevant information security legislation.

13.4 Data protection and privacy must be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. Key records must be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements. (See Appendix 5 and the School's Data Protection Policy).

PROTECTION OF DATA

13.5 The EPT and school will take appropriate steps to prevent, loss or incident, whether accidental or malicious, including error, fraud, damage and disruption to computing or communications facilities.

14 DEALING WITH INCIDENTS OF UNACCEPTABLE OR INAPPROPRIATE USE

SYSTEMS AND SECURITY MONITORING

14.1 All users should be aware that in order to provide a secure environment the following detective security controls are in place:

- The school email system is filtered and recorded
- Web usage is actively filtered and recorded
- System usage may be recorded

- System files, etc may be accessed to ensure confidentiality integrity and availability.
- All users are responsible for the security of ICT systems, including appropriate use of resources such as email and the internet.
- Parents and carers will be informed of the expectations and responsibilities of their child when using mobile ICT equipment and encouraged to support their child in fulfilling the expectations.
- Any user data retained by filtering systems will not be released unless authorisation has been given by the Headteacher or an appointed member of staff.

REPORTING

14.2 Any inappropriate or unacceptable use of the school ICT equipment, resources or personal devices during school time should be reported to the appropriate organisation.

CONSEQUENCES

14.3 EPT and the school reserves the right to suspend or terminate an account if a security breach is encountered. The unacceptable use will be investigated as a security incident and the school or EPT will decide on the appropriate disciplinary action.

- The Incidence Response Protocol is followed where inappropriate or illegal material may be present on school equipment
- Incidents are recorded in the correct section of the incident log by the Headteacher
- Internal Audit are informed of any potential security breach
- Appropriate investigations disciplinary procedures are followed.

14.4 School and the EPT reserve the right to suspend or terminate an account if a security breach is encountered. The unacceptable use will be investigated as a security incident and the school or EPT will decide on the appropriate disciplinary action.

14.5 Any violations of this security policy should initially be brought to the attention of the Headteacher. Violation of this security policy by a member of school staff may lead to disciplinary proceedings and/or legal proceedings against that individual. Intentional or persistent violation of this security standard by staff of third parties in a contractual relationship with the school, will be treated as a breach of the appropriate contract. Where a pupil is involved in intentional persistent violation of this policy, appropriate action will be taken by the Headteacher.

CONSEQUENCES RESPONSE INVESTIGATIONS

14.6 It is particularly important that all security and E-Safety incidents are logged and that a detailed record is kept of the investigation and resultant actions. All security incident reports and logs must remain confidential and only authorised personnel will be permitted to view this material. The investigation should, wherever possible, determine the extent of an incident, the impact of the incident, and the source of the incident. It may not always be possible to complete such investigations, but an attempt should be made to get far enough to make a reasonable recommendation as to actions that should be taken as a result of the incident.

14.7 The EPT or local law enforcement agency will be contacted if the severity of a security breach necessitates this course of action.

14.8 Investigations are normally conducted for all security incidents including but not limited to the following:

- Unauthorised access or an attempt to access a resource or other users account without approval.
- Unauthorised modification to systems whether successful or unsuccessful.
- Unauthorised disclosure of school information.
- Deliberate or unintentional hacking attempts.
- Rogue software or hardware appearing on the school network.

15 POLICY REVIEW

15.1 This policy will be reviewed by the Trust annually.

15.2 Due to the rapidly changing nature of technology, this policy may be updated more regularly as a result of advice from the EPT. Any changes should be shared with staff at the earliest possible opportunity.

APPENDIX 1 – STAFF INFORMATION SYSTEMS CODE OF CONDUCT

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's Acceptable Use Policy and E-Safety policy for further information and clarification.

- ICT equipment and software are the property of the school/EPT and I understand that it may be a criminal offence to use it for a purpose not permitted by its owner.
- I understand that I am responsible for my own use of new technologies, and will ensure that I use technology safely, responsibly and legally.
- I understand that school and personal ICT equipment may be used for private purposes out of school directed time only and that the use of school equipment may be monitored and should be in keeping with my professional status
- I understand that I must not use school ICT resources for personal financial gain, gambling, political purposes or advertising.
- I understand that my information systems and Internet use is subject to filtering and as such may be recorded.
- I will respect copyright and intellectual property rights. I will ensure that I have appropriate permissions before using or adapting work that may be the intellectual property of others and will acknowledge the source of all work that is not my own (See Appendix 5).
- I understand that it is my duty to protect my passwords and personal network login and should log off the network or lock the device before leaving it unattended.
- I will not install any software or hardware without permission.
- I understand my personal responsibility for safeguarding and protection of data and will comply with the data protection Act of 1998 and any other legal, statutory or contractual obligations that the school and EPT inform me are relevant (See Appendix 5).
- I will familiarise myself with the public sector information classification framework. This national Protective Marking System classifies information in the following three levels of classification: unclassified, protect and restricted (See Appendix 4).
- I will report any known misuses of technology, including the unacceptable behaviours of others to the Headteacher.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safeguarding to the designated senior person responsible for child protection.
- I will report any incidents of concern regarding suspected or actual failure of technical safeguards to the IT Department.
- I will ensure that any electronic communications with pupils are appropriate to my professional role.
- I will ensure that all electronic communications are written in a professional manner and understand that they are potentially public property.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to use ICT equipment and to the content they access or create.
- I understand that it is my duty to respect technical safeguards in place and will not attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services.

- I will take reasonable precautions to prevent damage to or loss of ICT equipment in my charge.

The school may exercise its right to record and monitor the use of the school's technology, including Internet access and email. The school will take the necessary action where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and will abide by the Information Systems Code of Conduct.

Signed: …….. Date: ……

Name in Capitals: ……..

Accepted for School:……..

Name in Capitals: …….. Date: ……..

APPENDIX 2 – PASSWORD SECURITY GUIDANCE

Staff should use a strong password and keep it confidential. Never write your password down or store it in a computer system. (A strong password contains a mixture of numbers, letters and punctuation)

- Never reveal your passwords to anyone (includes colleagues, Line Managers, family and friends)
- Never use the 'remember password' function.
- All users must prevent their username and password being used to gain unauthorised access by locking the workstation when it is not in use so that casual overlooking and unauthorised tampering is prevented.
- If you become aware, or suspect, that your password has become known to someone else, you must change it immediately where this is possible and report your concern to the Headteacher.
- Only use the user account to store data that is associated with the school.
- Users must not divulge their account passwords to others, must not permit others to use their accounts, and must not use accounts intended for the sole use of other individuals.
- Log off when leaving the room unattended. It is wise to save work before locking the workstation.
- Do not attempt to use your colleague's credentials.
- Where pupils have individual passwords, they should not share these with others and inform their teacher if they believe it has been compromised.
- Where pupils share a common login, they should be taught the importance of treating other pupils work with respect and keeping their group password secure.

APPENDIX 3 – ICT ASSET PROTOCOL

Where any ICT Asset (any school or EPT ICT equipment) is taken outside the site it must be checked out by the relevant person upon leaving the Site and checked in upon return.

Whilst any ICT Asset is outside the Site:

- the person who checked it out shall be responsible for taking all reasonable precautions and care of it and for its safe return;
- it shall not be left unattended in any place or vehicle (whether locked or unlocked) other than the residence of the person who checked it out;
- During Core Hours ensure laptops & any other digital equipment is secured when rooms are empty for extended periods other than school break periods. Outside Core Hours, when not in use, teacher/administrator laptops must either be locked out of sight or taken home by the member of staff.
- it shall not be used where there is any material risk of damage from liquids, impact or otherwise;
- it shall not be lent or entrusted to any other person;
- Any alleged theft shall be reported to the police and a crime reference number obtained and until the number is obtained it shall be deemed to be a loss rather than a theft.

In using any ICT Asset:

- users shall not attempt to modify or circumvent any antivirus or other security software;
- users shall not save any data to the Asset that may cause damage or interference or instability to the Asset or any part of the Asset, including any firmware, operating system or other software;
- Users shall comply with the Acceptable Use Policy when accessing the Wide Area Network.

Any person whom the school reasonably suspects may be in breach of this protocol may be denied permission to remove ICT Assets from the Site.

School shall ensure that any student or employee using ICT equipment out of school is aware of this protocol.

The School and Authority shall use reasonable endeavours to ensure that staff and students are informed of all further rules and procedures established from time to protect the security of ICT Assets.

Where any ICT Asset not on long term loan is taken outside the Site it shall be checked out by the relevant person upon leaving the Site and checked in upon return.

Users with devices on long term loan are responsible for returning the device to school on a regular basis, to ensure updates are installed.

APPENDIX 4 – INFORMATION CLASSIFICATION

Information classification is a means of standardising the way information is assessed, marked and handled according to how confidential it is. The national Protective Marking System to classify information and has been introduced throughout the public sector as the standard framework to allow the safe and appropriate sharing and protection of information. Please familiarise yourself with the following 3 levels of classification from the Protective Marking System, which are referred to throughout this Policy:

CONSEQUENCES

UNCLASSIFIED is the lowest level of classification and covers all information which can safely be shared or is already publicly available.

Information is UNCLASSIFIED if:

- It is intentionally publicly available
- Disclosure would not adversely affect any individuals, external organisations or the school
  e.g. School literature, the school website, press releases, all items of public record.

PROTECT

PROTECT is the first level of sensitive information. Information should be classified as PROTECT if "compromise of information would be likely to affect individuals in an adverse manner." The PROTECT classification should be used where disclosure would:

- Be likely to affect an individual or a small number of individuals in an adverse manner
- Cause substantial distress to an individual
- Breach proper undertakings to maintain the confidence of information provided by third parties (for example, breach commercial confidence with a supplier to the school).
- Breach statutory restrictions on the disclosure of information.
  E.g. documents/emails containing name, address, NI, DOB, commercial terms & conditions.

Most of the sensitive information which the school handles will be at the PROTECT level of classification.

RESTRICTED

RESTRICTED is a higher level of classification than PROTECT and is used where "compromise of information would be likely to affect the national interests in an adverse manner". The RESTRICTED classification should be used where disclosure would:

- Put an individual at significant risk of harm or long-term distress
- Release personal information for 1000 or more individuals that is not in the public domain, even if the information is not likely to cause harm or distress (i.e. the release of a large amount of PROTECT classified data relating to individuals).
- Significantly undermine public confidence in the Trust or other public body
- Cause widespread disruption to the work of the Trust or other local public sector
- Organisation
- Significantly impact the EPT and school's ability to discharge its duties under the Civil Contingencies Act

The RESTRICTED classification will apply to a small amount of data which the school handles, primarily relating to highly sensitive information on individual students and staff. E.g. documents/emails containing, name, address, NI, DOB, Salary, Pension, Benefit details, investigations, fraud etc.

APPENDIX 5 - DATA PROTECTION AND OTHER RELEVANT LEGISLATION

THE LEGISLATION

BACKGROUND

The responsibilities referred to in the previous sections recognise the requirements of the current legislation relating to the use of ICT systems, which comprise principally of :-

- General Data Protection Regulation;
- Data Protection Act 2018;
- Computer Misuse Act 1990;
- Copyright, Designs and Patents Act 1988

It is important that all staff are aware that any infringement of the provisions of this legislation may result in disciplinary, civil and/or criminal action.

The general requirements arising from these acts are described below.

GENERAL DATA PROTECTION REGULATION AND THE DATA PROTECTION ACT 2018

The General Data Protection Regulation and the Data Protection Act 2018 exists to regulate the use of computerised information about living individuals and gives rights to individuals about whom personal data is recorded (Data Subjects). They may obtain personal data held about themselves, should be told about the use of personal data and can expect it to be accurate. The act places obligations on those who record and use personal data (Data Users). They must follow sound and proper practices, known as the Data Protection principles. Principle 6, integrity and confidentiality, requires that security is in place during the collection, use and storage of personal data.

Any requests to view personal data must be in line with the GDPR and Access to Information procedures.

To be able to meet the requirements of the GDPR and the DPA, the Headteacher is required to compile a list of processing, giving details and usage of all relevant personal data held on computer within the school and notify the Information Commissioner of their processing. It is important that amendments are submitted where the scope of the system extends to new areas of operation. The GDPR and DPA 2018 are consistent with the principles established in the 1998 Act.

It is important that all users of personal data are aware of, and are reminded periodically of, the requirements of the act and, in particular, the limitations on the storage and disclosure of information.

Failure to comply with the provisions of the prevailing Act and any subsequent legislation and regulations relating to the use of personal data may result in prosecution by the Data Protection Registrar.

COMPUTER MISUSE ACT 1990

Under the Computer Misuse Act 1990 the following are criminal offences, if undertaken intentionally:

- Unauthorised access to a computer system or data;
- Unauthorised access preparatory to another criminal action;
- Unauthorised modification of a computer system or data.

All users must be given written notice that deliberate unauthorised use, alteration, or interference with a computer system or its software or data, whether proprietary or written 'inhouse', will be regarded as a breach of school policy and may be treated as gross misconduct and that in some circumstances such a breach may also be a criminal offence.

The Copyright, Designs and Patents Act 1988 provides the legal basis for the protection of intellectual property which includes literary, dramatic, musical and artistic works. The definition of "literary work" covers computer programs and data.

If an organisation is using illegal copies of software the organisation may face not only a civil suit, but corporate officers and individual employees may have criminal liability. If liability is proven this could lead to an unlimited fine and up to ten years imprisonment per offence.

Where computer programs and data are obtained from an external source, they remain the property of the originator. Our permission to use the programs or data will be governed by a formal agreement such as a contract or licence.

All copying of software is forbidden by the Act unless it is in accordance with the provisions of the Act and in compliance with the terms and conditions of the respective licence or contract.

All users must be given written notice that failure to comply with the provisions of the Act will be regarded as a breach of school policy and may be treated as gross misconduct and may also result in civil or criminal proceedings being taken.

THE REGULATION OF INVESTIGATORY POWERS ACT 2000

The Act specifies that communications may be monitored and recorded for "a legitimate purpose" such as system and employee performance monitoring; detection and prevention of crime; detection of unauthorised use (including unauthorised use by employees; protecting against hackers and viruses; and ensuring the Council is complying with regulatory or self-regulatory practices or procedures relevant to the business.

Monitoring can only be carried out legally if the organization concerned has informed its staff that it is undertaking monitoring for these purposes. The provisions of the RIP Act have been taking into account in the formulation of Council policy relating to email and telephone use as detailed later in this document. Consistent with the EPT and school policies for Misconduct and Workplace Harassment and Equal Opportunities, non-adherence to this policy may result in disciplinary action being taken by the Trust that may result in dismissal and/or Civil or Criminal Court action.

APPENDIX 6 - UNACCEPTABLE USE

This section does not provide a complete list of usage and behaviours that are considered unacceptable, but it gives some examples of unacceptable use, in order to help all users of the ICT Service to make decisions on unclear areas.

The following activities will always be considered unacceptable use of the school ICT environment by any user:

- Development, or deliberate release, of rogue code (i.e. viruses, trojans, etc.).
- Interference with the work of other users (e.g. altering or copying their work).
- Grooming (including for political, extremist purposes).
- Hacking, probing, scanning or testing the weaknesses of a system within the school ICT environment, or on the Internet. Unauthorised access to systems. Violating or attempting to violate the security of the network.
- Actions that bring the school, or the school's ICT environment, into disrepute, or that are likely to do so.
- Deliberately wasting resources (e.g. unnecessary copying or emailing or very large files).
- Use of the environment for personal financial gain.
- Any illegal activity, including breach of copyright.
- Attempting to log on using another person's username and password.
- Making your username and password known to any unauthorised person.
- Creating or storing offensive, intimidating, insulting or harassing material on the school network.
- Accessing data not intended for you to access.
- Attempting to bypass filtering, or to access inappropriate or illegal material – such attempts will be reported to the school authority.
- Leaving your workstation logged in while unattended.
- Connecting additional devices to data points on the ICT network without specific agreement.
- Attempting to interfere with services to any user, host or network.
- Taking any action in order to obtain services to which you are not entitled.
- Conducting any unlawful or illegal activity.
- Using the services to create, transmit, distribute or store content that invades the privacy or other personal rights of others.
- Assisting, encouraging or permitting any persons in engaging in any of the activities described in this section.
- Sending email messages which result in complaints from the recipient or from the recipient's email provider, or which result in blacklisting of the sender's email address or mail server.
- Sending email or messages which are excessive and/or intended to harass or annoy others.
- Sending, or attempting to send, spam of any kind from third-party networks using a return email address that is hosted on the ICT mail servers or referencing an email address hosted on the ICT mail systems.
- Failing to observe intellectual property.
- Keeping, accessing or transmitting confidential data about other students.
- Producing documents or emails that contain obscene, offensive, unlawful, intimidating, defamatory, harassing, abusive, fraudulent, or otherwise objectionable content as reasonably determined by the school or EPT.

- Causing technical disturbances to ICT systems by introducing viruses of any kind.
- Any use that interferes with, or prevents, another user's permitted use of the environment.
- Unauthorised modification or reconfiguration of school's ICT systems.
- Using managed service email or messaging systems to engage in inappropriate or nonprofessional communications between staff, staff and students or students
- Any uses of school ICT equipment of personal equipment connected to the network, intended to bully or harass others.

APPENDIX 7 - GLOSSARY OF CYBER SECURITY TERMINOLOGY

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

term	definition
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.

term	definition
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.