Information Security Policy

Applicable to:	✓	All individual schools within NEAT Academy Trust
	×	Specified schools only within NEAT Academy Trust
	✓	Central Team within NEAT Academy Trust
	✓	NEAT Active Ltd
Approval body:	NEAT Academy Trust Finance, Audit and Risk Committee, which may be delegated NEAT Active Ltd Board of Directors, which may be delegated	
Effective from:	The transfer from an externally managed IT service to an in-house IT service i.e. • 1 April 2022 for St Hild's Church of England School • 1 September 2022 for NE6 schools, NEAT Central Team and NEAT Active Ltd	

Status:

Statutory policy or document	No
Review frequency	As determined by the Boards
Approval by	As determined by the Boards

Publication:

Statutory requirement to publish on website	No
If not, agreed to publish on website?	Yes – trust and school websites

Version Control:

Revision Record of Issued Versions			
Author	**Creation Date**	**Version**	**Status**
Head of Digital Resources and Delivery (SD)	3 April 2022 by FAR Committee for NEAT 3 May 2022 by NEAT Active Board	1.0	New policy to ensure appropriate information security management for the in-house IT service.
Changed by	**Revision Date**	**Version**	**Status**

Review Date	
Frequency	**Next Review Due**
Every three years	April 2025 (or earlier if new guidance or legislation issued and/or business need for earlier review identified)

1 Purpose

Information is one of our most important assets. The purpose of this policy is to define the information security processes and standards we will implement to ensure that we:

- meet our obligations to protect the personal data we process through the implementation of appropriate technical and organisational measures;
- maintain confidentiality – access to data will be restricted to those with specific authority to view the data in question;
- maintain integrity – information will be complete and accurate; and
- maintain availability – information will be available and delivered to the right person when it is needed and in accordance with the relevant statutory provisions.

2 Scope

This policy applies to both NEAT Academy Trust and its subsidiary company, NEAT Active Ltd (the NEAT Group).

It applies to information in all forms including, but not limited to:

- hard copy or documents printed or written on paper;
- information or data stored electronically, including scanned images;
- communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- speech, voice recordings and verbal communications, including voicemail;
- published web content, for example internet and intranet;
- photographs and other digital images.

The UK GDPR and Data Protection Act (2018) apply to personal data, however the companies also process large volumes of non-personal data as part of their operations and this data is also an important business asset. While personal data requires special consideration, the principles of confidentiality, integrity and accessibility are also applicable to other business information processed by the companies and the measures outlined in this policy should be used as necessary when processing such information.

This policy should be read in conjunction with the:

- Data Protection Policy and Personal Data Breach Procedure
- Freedom of Information Policy
- Surveillance Policy specific to relevant schools/services
- Acceptable Use Protocols
- Records Management and Retention Policy

3 Policy statement

We process large volumes of information, including personal data, to deliver our core objectives. It is essential that our information systems and data networks are adequately protected from events which may compromise the information held or the carrying on of our business. To this end we are committed to developing and maintaining an information systems structure which has an appropriate level of

security.

We will maintain the security and confidentiality of personal data and all other information in both paper and electronic formats, held by it, its information security systems and relevant applications and networks by:

- ensuring appropriate technical and organisational measures are in place to prevent unauthorised access, damage or interference to and/or with information, ICT assets and network services;
- ensuring that we are aware of, and comply with the relevant legislation;
- creating a culture where information security principles become an integral part of how we conduct our business;
- ensuring all stakeholders understand their individual and collective responsibilities, and the implementation of information security principles within each setting.

Risks to information security have been identified using the approach to assessing risks outlined in the Risk Management Policy. Physical, technical, and organisational measures to control those risks are described in this policy. These measures apply to all schools/services, unless stated otherwise.

Variations in context between schools/services may affect the specific solution required to implement a measure and the policy identifies where individual schools/services can choose the most appropriate control from the range described. Some control measures have a range of solutions with a minimum essential requirement and then further additional protections that the school/service may choose to implement.

4 Legal considerations

This policy is designed to comply with the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

Failure to ensure adequate security and protection of information may lead to:

- legal action against the company and/or the individual responsible for the breach. Such legal action could include an investigation by the Information Commissioner's Office (ICO) who can impose significant financial penalties and/or a claim for damages for breach of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018);
- irreparable damage to confidence in the companies and individual schools/services.

5 Roles and responsibilities

- **NEAT Academy Trust and NEAT Active Ltd Boards of Directors:** The Boards will review this policy and evaluate its effectiveness (the NEAT Academy Trust Board delegates this to its Finance, Audit and Risk Committee). The Committee has oversight of any risks arising from information governance.

- **Information asset owners (IAO):** An IAO is the individual responsible for an information asset, understands the value of that information and the potential risks associated with it. IAOs will be appointed based on sufficient seniority and level of responsibility. IAOs are responsible for the security and maintenance of their information assets. This includes ensuring that all colleagues are using the information safely and responsibly. They will also determine the retention period for the asset, and when destroyed, ensure this is done so securely.

- **Data Protection Officer (DPO):** The Data Protection Officer appointed for the NEAT Group is: Veritau Ltd, Information Governance Team, County Hall, Racecourse Lane, Northallerton DL7 8AL Tel: 01609 554025 E-mail: schoolsDPO@veritau.co.uk . The DPO is a statutory position and operates in an advisory capacity. Their duties include:
  - acting as the point of contact for the Information Commissioner's Office (ICO) and data subjects;
  - facilitating a periodic review of the corporate information asset register and information governance policies;
  - assisting with the reporting and investigation of information security breaches;
  - providing advice on all aspects of data protection as required, including information requests, information sharing and Data Protection Impact Assessments; and
  - reporting to non-executive directors/trustees on the above matters.

- **Head of Digital Resources and Delivery:** The Head of Digital Resources and Delivery is responsible for all aspects of security risk for IT and cyber security. The scope of this role covers all security technologies and services, including the implementation of IT and cyber security management.

- **All employees and authorised agents acting on behalf of NEAT Academy Trust or NEAT Active Ltd (as defined below):** have a duty to ensure they understand and comply with this, and other related policies listed in section 2 of this policy. Failure to comply with this policy by employees may be dealt with under the NEAT Group's Disciplinary Procedure and could include dismissal from employment. Failure to comply with this policy by authorised agents (including volunteers, agency workers and contractors) could result in the end of the arrangements for their services.

6 Definitions

"The Companies" means NEAT Academy Trust and NEAT Active Ltd.

"The Trust" means NEAT Academy Trust, which operates the network on behalf of both companies. The ICT network consists of both hardware and software held within the trust.

"Users" means all employees (whether employed directly by the company or on its behalf by a local authority or other employer) and any authorised agents working on behalf of the company, including temporary or agency staff, governance/other volunteers, and third-party contractors

"Data protection legislation" means the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

"Data" means personal data and special category personal data as defined by the data protection legislation, and confidential and sensitive information held by the company.

"Personal data" any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification

number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Special category/sensitive personal data" means information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.

"Processing" means any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.

"Data subject" means all living individuals about whom the company holds data. A data subject need not be a UK national or resident. All data subjects have legal rights in respect of their data and the information that the company holds about them.

"Subject access request" ("SAR") means a request by a data subject to access the data the company holds about them under Article 15 of the GDPR.

"Information Asset" means data held by the company in any form. This data may be held electronically by software in computer systems and transferred across a network, on paper, in files or transferred by post, courier or in person.

"Information Asset Owner" ("IAO") Information Asset Owners are senior members of staff who have been appointed to be responsible for one or more identified information asset(s). This person will be responsible for ensuring that the information asset is accurately stored and maintained on the information asset register.

"ICO" means the Information Commissioner's Office.

"Information security" means The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability.

"Information security breach" means a breach which may be caused by a technical failure, unauthorised access to either the trust's network or a client device used for company business by a third party, loss of the company's information and/or inappropriate actions of an individual or individuals which result in the compromise of information belonging to or held by the company.

"Information security vulnerability" means an identified weakness of a system(s) or process that puts the security and availability of information at risk.

"Client device" means laptops, tablets, telephones, smartphones, desktop computers or other electronic equipment that could be used for the carrying out of company business or the processing or storing of information.

"Personal device" means a client device not directly owned by the company.

"Username" means a unique sequence of characters used to identify a person,

system or service, allowing access to a computer system, computer network, client device, or online account.

"Strong password" means a phrase of sufficient random characters to prevent guessing or brute-force attacks. A strong password must be a minimum of 8 characters, does not use single common number sequences/dictionary words or easily accessible personal information (i.e., any portion of your name, date of birth, telephone numbers or NI numbers). Strong passwords of less than 24 characters must include a combination of three of the following: lowercase and uppercase letters, numbers and symbols.

"Secure authentication device" means a device or component integrated into a client device that allows the encrypted storage and retrieval of strong passwords using biometric information.

"Two-Factor Authentication (also known as Multi-Factor Authentication, MFA or 2FA)" means a method of confirming a claimed identity using a combination of at least two of the following categories: knowledge (something they know, e.g., a password), possession (something they have e.g. a token), and inherence (something they are e.g. a fingerprint).

"Authorised user" means a person, or administrative service, that is authorised by the company to authenticate to a system that may contain data and potentially to receive authorisation to access resources provided by or connected to that system.

"Removable media" includes USB sticks, external hard drives, CD's or other media which can be connected to the Trust network or a client device and used for storing information.

"External" means any and all buildings, systems or services not directly owned by the company, including all accounts not ending in neat.org.uk

"Social media" means websites and applications that enable users to create and share content or to participate in social networking including Facebook, LinkedIn, Twitter, Google+, and all other social networking sites, internet postings and blogs. It applies to use of social media for company purposes, as well as personal use that may affect the company in any way.

"Cloud service" means cloud computing/service is the delivery of computing resources using a network of remote servers hosted on the internet to store, manage, and process data, rather than local servers or a personal computer.

7 Use of client and personal devices

Client devices used for, or in connection with, company business and in particular for the collection or storing of personal data and/or special category personal data must be kept secure with strong passwords. If available with the device, an approved secure authentication device to aid entering of the password should be used.

Client devices used for, or in connection with, company business must not be left unattended in plain sight at any time, including whilst at home or travelling, and must be protected against loss, damage, misuse or unauthorised access. When not in use, client devices must be stored in a secure, lockable location and should never be stored in vehicles, even if locked.

Client devices used for, or in connection with, company business must not be used to access, view or process personal data or special category personal data in a manner that allows anyone other than the authorised user to view the data.

Personal devices, including but not limited to, laptops, tablets, telephones, smartphones, desktop computers or other electronic equipment, must not be used to store data.

Client devices used for, or in connection with, company business must be updated with the manufacturer's software and other updates regularly when updates become available, and where supported have antivirus software installed and regularly updated.

Client devices used to store personal data or special category personal data will be encrypted.

Client devices issued to a user for or in connection with company business by the Trust must only be used by the user. At no time shall any other user, including but not limited to, family members, friends, and employees from another organisation, be permitted to use the device.

If a client device used for, or in connection with company business is lost or stolen, the loss/theft should be reported to the Head of Digital Resources and Delivery as soon as possible (further escalation will be reviewed on a case-by-case basis) and in any event within 24 hours of the loss/theft occurring. Where possible the client device should be remotely accessed, and the information erased.

Control measures detailed in sections 7.1 to 7.3 are deemed essential.

7.1 Personal devices and personal data

- Personal devices must not be used for accessing, storing, or creating personal data.

- Where a user believes they have legitimate need to process personal or special category data using a personal device they should contact their line manager with a business case for provision of a client device.

7.1.1 **Inventory of equipment and devices**

The IT support team will maintain an inventory of equipment and devices that are owned, and records of client devices issued to users.

7.1.2 **Personal email accounts**

Users must only use email accounts provided by the company to carry out business on behalf of the company. Users must not use personal email accounts to access or transmit personal data.

7.2 Cloud computing

- Only cloud computing networks or services, including social media commissioned by the company or expressly authorised by the Head of Digital Resources and Delivery, may be used to store and send information concerning or relating to company business. The use of personal cloud storage solutions (SkyDrive, OneDrive Personal, iCloud, G-Drive etc.) for the

transfer of company information is expressly forbidden.

- Personal data, special category personal, confidential and sensitive information, whether on the trust's network or a client device must not be stored on a cloud computing network or service not commissioned by the Trust, or expressly authorised by the Head of Digital Resources and Delivery.

- If data or other information concerning or relating to company business is to be stored in or on a cloud network, the company will take all reasonable steps to find out in which country the Data or other information is being stored, and to ensure that appropriate measures are in place in relation to any data transferred outside of the EEA.

- If the company receives notification that data in respect of company business has been corrupted, lost or otherwise compromised while stored on a cloud network, the company should ascertain whether any or all of the information stored in the cloud can be recovered and if this is possible restore that information;

- Any corruption, loss or compromise of information held on a cloud network should, if appropriate, be reported via the mandatory reporting procedure set out at section 12 of this Policy.

7.3 Removable media

The use of removable storage is prohibited across the trust's network. All users are directed to use Google Drive/Google File Stream to share and access data securely.

8 Securing information

The IT support team will maintain an Information Asset Register detailing which individuals have access to which systems (both electronic and manual). Control measures detailed in sections 8.1 and 8.2 are deemed essential.

8.1 Physical access controls

8.1.1 **Manual filing systems**

Access to manual filing systems (i.e. non-electronic systems) will be controlled by a key management system. All files that contain personal data will be locked away in lockable storage units, such as a filing cabinet or a document safe, when not in use. Access will only be given to individuals who require it to carry out legitimate business functions.

8.1.2 **Clear desk policy**

Individuals will not leave personal data on desks, or any other working areas, unattended and will use the lockable storage units provided to secure personal data when not in use.

8.1.2 **Alarm system**

The school/service will maintain a security alarm system at its premises so that, when the premises are not occupied, an adequate level of security is still in operation.

8.1.3 **Building access**

External doors to the premises will be locked when the premises are not occupied. Only authorised users will be key holders for the building premises.

8.1.4 **Internal access**

Internal areas, which are off limits to pupils/service users and visitors, will be kept locked. Acceptable access control measures are:

- PIN numbers
- Electronic fob system
- Keys

The ICT Infrastructure Manager is responsible for the access management system.

8.1.5 **Visitor control**

Visitors to the premises will be required to sign in and wear a visitor's badge. Visitors will be escorted throughout the site and will not be allowed to access restricted areas without supervision.

8.1.6 **Siting of devices**

User workspaces will be arranged such that members of the public cannot read from computer monitors or overlook paper records.
Users processing personal, and especially special category, data should have workstations that are not overlooked by people without authority to access such data.

8.2 Password and access control

Access to data stored electronically must be controlled through the use of a strong password.

Access to authorised user accounts must be controlled, as a minimum, through the use of a password, which must not be less than 8 ASCII characters in length. Where a system or service provides alternative authentication methods, including but not limited to, facial or biometric recognition, the alternative authentication method must be in addition to a password.

Users must ensure that they have a strong password for all authorised user accounts and the same password not re-used across different types of system.

Users must ensure that all passwords are changed from the default password.

Authorised users are responsible for keeping their assigned password(s) secure and must ensure their password(s) is neither disclosed to, nor used by, anyone else under any circumstances.

Use of another person's username or password will constitute an information security breach and must be reported in accordance with the procedures set out in this policy, and the Data Protection Policy.

Authorised users are responsible for ensuring that all devices used to access company data or other confidential information, are logged off, switched off or otherwise controlled by a strong password when unattended or not in use, at all times.

Authorised users with access to the trust's network which is used for, or in connection with company business are responsible for any actions carried out under their username and password.

Where available, users using critical systems or accessing personal or special category personal data should use two-factor authentication.

Two factor authentication is enabled on all IT support team accounts and those who have admin access to Google services.

8.2.1 **Electronic systems**

Access to electronic systems is controlled through a system of user authentication. Individuals will be given access to electronic systems if this is required to carry out legitimate functions. A two-tier authentication system will be implemented across all electronic systems. The two tiers will be username and unique password.

Individuals will be required to change their password every 90 days. Usernames will be suspended either when an individual is on long term absence or when an individual leaves the company.

No user is permitted to log onto any other user's account - in the (unlikely) event of a requirement to access another user's account; this must be requested via the IT support team.

Users must:

- lock their screen using CTRL+ALT+DEL when away from their workstation;
- log off from the network and shutdown PCs every night unless asked not to by the IT support team;
- report any suspected breaches of password security to IT support services.

8.2.2 **Surveillance systems**

CCTV and e-monitoring software are used across the trust. Due to the sensitivity of information that could collected as a result of this operation, each school/service has a separate policy which governs the use of surveillance equipment.

8.2.3 **Software and systems audit logs**

All software and systems should (where possible) have inbuilt audit logs so that it is possible to monitor what information users have accessed and what changes may have been made. Although this is not a preventative measure, it does ensure that the integrity of the data can be assured and also deters individuals from accessing records without authorisation.

8.2.4 **External access**

On occasions the school/service will need to allow individuals who are not employees to have access to data systems. This could be, for example, for audit purposes, to fulfil an inspection, when agency staff have been brought in, or because of a partnership arrangement. The IAO is required to authorise all instances of third parties having access to systems. Details of external access to systems (who has been given access to what systems,

reasons for, and who authorised the access) will be maintained as part of the Information Asset Register.

8.2.5 **Shared drives**

Schools/services maintain a shared drive on its servers. Users are encouraged not to store personal data on the shared drive, but it is recognised that on occasion there will be a genuine business requirement to do so.

Users must adhere to any defined file naming protocols and filing structures in the record management plan so that personal data can be easily identified in the event of a subject access request and managed within the appropriate retention guidelines.

Access to and within the shared drive should be restricted to users with a business need to access the information: for example, a HR folder in the shared drive should be accessible only to users responsible for HR matters. The IAO must give permission for shared drive access rights to users. Shared drives are subject to the Records Management and Retention Policy.

8.2.6 **Leaving the company**

Upon leaving, users must return/transfer, in a useable format, all equipment and information including data to the trust, on or before their leaving date (e.g., last day of employment) to their line manager, or other company representative.

This includes, but is not limited to:

- all information, including data, used or stored as part of the role, both physical and electronic;
- all information, including files, documents and emails, including any data, stored within individual cloud service accounts;
- client devices loaned by the company including PIN numbers, usernames or passwords required to reuse or reset the devices;
- any removable devices provided by the trust;
- access control, PIN, tokens and ID cards;
- keys and PIN numbers used to access physical locations.

After leaving users must not attempt to access or use any company information, including any data. User accounts for staff in schools are disabled automatically based on the set end date within the school's MIS.

8.2.7 **Physical server access**

Physical access to servers and server rooms is restricted to authorised members of the IT support team. Where feasible, access control measures to server rooms are in place and access is logged. Server rooms are kept locked at all times. Cabinets containing servers are kept locked at all times and only authorised members of the IT support team can gain access.

9 Remote working / working offsite

9.1.1 **Working offsite**

It is understood that users may need to work at home or away from the company premises. For some users (e.g. governance volunteers) this will be on a regular basis. Where this is the case, then the users will adhere to the following:

Essential controls:

- Users must make sure personal data or company devices are secured if left unsupervised at home for extended periods of time (for example when the user goes on holiday).
- Users must not keep personal data or company devices in cars if unattended.
- Private working area - Users must not work with personal data in areas where other individuals could potentially view or even copy the personal data (for example on public transport).
- Users must take care to ensure that other household members do not have access to personal data and do not use company equipment for their own personal use.
- Trusted Wi-Fi Connections - Users will only connect their client devices to trusted Wi-Fi connections and will not use 'free public Wi-Fi' or 'Guest Wi-Fi'. This is because such connections are susceptible to malicious intrusion.
- When using home Wi-Fi networks users should ensure that they have appropriate anti-virus software and firewalls installed to safeguard against malicious intrusion. If in doubt users should seek advice assistance from the IT support team.
- Data removal and return -Users will only take personal data away from the company premises if this is required for a genuine business need. Users will take care to limit the amount of data taken away from the premises.
- Personal data should be anonymised or pseudonymised before removal from the company premises wherever practicable.
- Users will ensure that all data is returned to the company premises either for re-filing or for safe destruction. Users will not destroy data away from the premises as safe destruction cannot be guaranteed.

Additional (optional) controls:

- If users are working at home, they will ensure that they have lockable storage to keep personal data and company equipment safe from loss or theft. If the user does not have access to lockable storage, then they may apply to the school/service for assistance in purchasing such storage.

9.1.2 **Remote access to company IT systems**

Users should remotely access personal data on the trust's network rather than downloading personal data to corporate devices (including encrypted storage devices).

Essential controls:

- When using remote access users must make sure the device is locked when left unattended.
- Remote access to ICT systems or resources must connect using an approved method using multi factor authentication. (For example - Username, password and token or pin)
- Approval for remote access user set-up must be given by the IAO.

The school may utilise MIS systems which are cloud-hosted and accessed via an internet portal (e.g. CPOMS). If these systems will include personal data, IAO's must ensure that a data protection impact assessment is completed prior to the transfer of any personal data. Access to these systems via external network connections should be avoided wherever possible and should be limited to users authorised by the IAO.

10 Storing and transportation of non-electronic data

Data can be vulnerable to loss, unauthorised access, misuse or corruption when being physically transported either personally by users or when sending data via the postal service or couriers.

Special controls should be adopted where necessary to protect data from unauthorised disclosure or modification and may include:

- ensuring the packaging is sufficient to protect the contents from any physical damage likely to arise in transit;
- delivering by hand records containing personal data, where appropriate;
- sending data via secure post such as Royal Mail recorded or signed for delivery or special delivery or as otherwise agreed with the data subject;
- records containing special category personal data shall not be delivered by hand unless absolutely necessary. In which case the following should occur:
    - documents transported in vehicles should be hidden away or placed in boot where possible, and the vehicle locked;
    - documents should never be left unattended, even in a locked vehicle.

Consideration should be given to the necessity of transporting or moving data or other records as this increases the risk of data loss.

11 Transportation/transmission of electronic data

Personal data, special category personal, confidential and sensitive information sent or transmitted externally using electronic systems or services must be secured using a process that ensures the data is encrypted and users must carefully check the recipient's contact details before sending.

Data must only be sent or transmitted externally when authorised by job description, company policy, applicable legislation, or when specially authorised by the IAO. The sending of personal data and special category personal data to personal cloud systems or services email accounts is expressly forbidden. Users working remotely are required to access data through the company's authorised systems and services.

Data must not be sent using any systems or services, including but not limited to, cloud platforms and social media providers or any other type of system not owned by the company, including text messaging.

Personal data and special category personal data must be sent to named users only. Multi-user posting, sending or transmission, including, but not limited to, email lists, distribution groups, security groups, chat/team-based groups, forums, rooms and channels is prohibited.

12 Information security incident reporting and management

The companies will have and maintain a register where all information security incidents are logged. This log as a minimum should include:

- the nature of the breach;
- the number of information assets compromised;
- how the Information Asset(s) has/have been compromised;
- whether any special category personal data was compromised;
- whether the incident needs to be reported.

Where there has been any breach the Head of Digital Resources and Delivery must be informed immediately, so they can decide if an information security breach has occurred and in order that consideration can be given to reporting the breach to the appropriate authorities.

If there has been an information security breach but it does not involve the compromise of more than one record, it should be recorded in the Information Security Incident Log.

Examples of an information security breach include but are not limited to:

- password(s) written down or stored, in an accessible, plain text or otherwise visible, manner to persons other than the authorised user;
- using another person's password;
- divulging of a password;
- making use of personal data for personal gain;
- accessing data for personal knowledge;
- attempting to gain access under false pretences;
- unauthorised release of data;
- knowingly entering inaccurate data;
- deleting data prior to the retention period or any other period set out in the Records Management and Retention Policy expiring;
- loss or misuse of data;
- malicious damage to equipment or data;
- changing permissions that allows access to, or sharing information (including data) with, persons not authorised to access the information;
- unauthorised removal of data, company equipment or equipment used for or in connection with company business from company premises or another site authorised for the storage of such information or equipment;
- loss or theft of a client device used for or in connection with the company and/or for company purposes or any other device belonging to the company.

13 Business continuity

13.1 Environmental security

As well as maintaining high standards of physical security to protect against unauthorised access to data, the trust must also protect data against environmental and natural hazards such as power loss, fire and floods.

It is accepted that these hazards may be beyond the control of the trust but mitigating controls will be implemented:

Essential controls:

- Back-ups – the IT support team is responsible for creating and managing back-ups so that should the company's electronic systems be compromised then the service provider will be able to reinstate the data from the backup with minimal destruction.
- Fire alarm system – schools/services will maintain a fire alarm system to alert individuals of potential fires and so the necessary fire protocols can be followed.
- Fire doors - areas of the premises which contain paper records or core electronic equipment, such as server boxes, will be fitted with fire doors so that data contained within those areas will be protected, for a period of time, against any fires that break out on the premises. Fire doors must not be propped open unless automatic door releases are installed.

Additional (optional) controls:

- Fireproof cabinets - only lockable data storage cabinets that can withstand exposure to fires for a short period of time will be purchased. This will protect paper records held in the cabinets from any minor fires that break out on the building premises.

13.2 Systems security

The companies recognise that the loss of, or damage to, IT systems could affect their ability to operate and could potentially harm pupils/service users and other stakeholders. The following systems security controls will be implemented:

Essential controls:

- Software Download Restrictions - the IT support team will manage the download and installation of all software. Users cannot directly download software on to the company's IT systems. The IT support team will vet software to confirm its security certificate and ensure the software is not malicious.
- Phishing emails - Users must not click on links that have been sent to them in emails when the source of that email is unverified. Users will also take care when clicking on links from trusted sources in case those email accounts have been compromised. Users must check with the IT support team if they are unsure about the validity of an email.
- Firewalls and anti-virus software - The IT support team will ensure that firewalls and anti-virus software are installed on electronic devices and routers, and review and update this so that the protection is fit for purpose. Individual users are responsible for ensuring that any portable devices issued to them are updated in line with the device agreement.
- Personal devices - Personal devices must not be physically connected to the trust network.
- System updates – All system updates (for example - patches, operating system, application updates) will be implemented by the IT support team within relevant timescales.

14 Disposal of data and equipment

14.1 Disposal of waste

Disposal of waste will be made with due regard to the sensitivity of the information they contain. If personal data or other confidential information is included the following controls will be implemented:

Essential controls:

- Paper records will be securely destroyed by either:
  - the use of cross-cutting shredders
  - a secure confidential waste management service.
- Electronic records should be deleted in line with the appropriate retention period in the Records Management and Retention Policy with care that emails must also be removed from the 'Deleted Items' folder.
- A destruction log will be maintained as part of the records management system.

14.2 Repair and disposal of ICT equipment

Repair and disposal of all ICT equipment owned by the company (including

removable media) must only be carried out by the trust's IT support team. The company has ensured that appropriate clauses are contained within the service agreement to meet the requirements of the Data Protection Act.

15 Training

Data protection information and training is provided for all users as part of induction to the organisation and subsequently as an annual refresher. This will include:

- Acceptable Use Protocol
- Information Security Policy
- Personal Data Breach Procedure
- Data protection: rights and responsibilities.

Each school/service provides:

- annual refresher training in data protection
- suitable training for all ICT users and documentation to promote the proper use of ICT systems
- information on records management protocols in their school/service.

A record of the training provided to each individual user will be maintained at each school/service.

General

This policy is at the discretion of the Boards of Directors and can be varied at any time. In the event of any conflict with primary legislation or statutory regulations, the legal provisions will have precedence over this policy in all cases.