

INFORMATION SECURITY POLICY

Status: Statutory

Updated: May 2024

Reviewed and ratified by: SECAT Executive Team

Signed by CEO.....



Next review date: May 2025

Published location: www.secat.co.uk



Introduction

In May 2018 the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) became enforceable across the United Kingdom.

The Information Security Policy outlines the school's organisational security processes and standards. The policy is based upon the sixth principle of the GDPR which states organisations must protect the personal data, which it processes, against unauthorised loss by implementing appropriate technical and organisational measures. This policy has been written using the security framework recommended by ISO: 270001 (internationally recognised Information Security Standard).

This policy should be read in conjunction with the other Data Protection suite policies

Scope

All policies in the Data Protection suite apply to all **Trust** employees, any authorised agents working on behalf of the **Trust**, including temporary or agency employees, and third party contractors.

Individuals who are found to infringe these policies knowingly or recklessly may face disciplinary action.

The policies apply 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 intranet and internet,
- Photographs and other digital images.

Access Control

The **schools** will maintain control over access to the personal data that they process.

These controls will differ depending on the format of the data and the status of the individual accessing the data. The **schools** will maintain an audit log detailing which individuals have access to which systems (both electronic and manual). This log will be maintained by the **Headteacher**, who may delegate to a member of their team.

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.

Keys to storage units will be stored securely. The Headteacher of the individual school will be responsible for giving individuals access. Access will only be given to individuals who require it to carry out legitimate business functions. Where a PIN is used, the PIN will be changed every academic year or whenever a member of staff leaves the organisation, or if there is any suspicion the PIN has become known to any unauthorised person, whichever is sooner.

Electronic Systems

Access to electronic systems will be controlled through a system of user authentication. Individuals will be given access to electronic filing systems if 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. Multi factor authentication will be used wherever this is supported.

Individuals will be required to change their password on a regular basis and usernames will be suspended either when an individual is on long term absence or when an individual leaves employment of the school.

Software and Systems Audit Logs

The Trust will ensure that all major software and systems have inbuilt audit logs where applicable so that the Trust can ensure it can monitor what employees and 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.

Data Shielding

The Trust does not allow employees to access the personal data of family members or close friends. Employees should declare, upon employment, whether they are aware of any family members or friends who are registered at SECAT.

The schools will then ensure that the declaring employee cannot access that data.

Employees who knowingly do not declare family and friends registered at the Trust may face disciplinary proceedings and may be charged with an offence under Section 170 of the Data Protection Act 2018 (unauthorised access to information).

External Access

On occasions the Trust will need to allow individuals who are not employees of the Trust 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 with another Trust. The Headteacher is required to authorise all instances of third parties having access to systems. If the above individual is not available to authorise access, then access can also be authorised by the Headteacher's nominated person or a more senior individual at the Trust.

An access log, detailing who has been given access to what systems and who authorised the access, will be maintained by the schools.

Physical Security

The Trust will maintain high standards of Physical Security to prevent unauthorised access to personal data. The following controls will be maintained by the schools:

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.

Alarm System

The Trust 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.

Building Access

External doors to the premises will be secured when the premises are not occupied. Only authorised employees will be key holders for the building premises. The Headteacher, who may delegate to a member of their team, will be responsible for authorising key/access credential distribution and will maintain a log of key holders.

Internal Access

Internal areas that are off limits to pupils and parents will be kept secured and only accessed through PIN, ID card keys. PINs will be changed every academic year or whenever a member of staff leaves the organisation, or whenever there is a suspicion an unauthorised individual is aware of the PIN. Keys will be kept in a secure location and a log of any keys issued to staff maintained.

Visitor Control

Visitors to the schools will be required to sign in to the site via the school's signing in system and state their name, organisation, car registration (if applicable) and nature of business. This may be either in paper or electronic format. Visitors will be escorted throughout the school and will not be allowed to access restricted areas without employee supervision.

Any physical visitor books will be locked away at the end of the working day and kept for current financial year + six years.

Environmental Security

As well as maintaining high standards of physical security, to protect against unauthorised access to personal 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 the Trust will implement the following mitigating controls:

Back Ups

The individual schools will back up their electronic data and systems on a regular basis. If these backups are kept off site by an external provider, this arrangement will be governed by a data processing agreement. Should the school's electronic systems be compromised by an environmental or natural hazard, then the Trust will be able to reinstate the data from the backup with minimal destruction.

Fire Proof Cabinets

Moving forward the Trust will aim to only purchase lockable data storage cabinets that can withstand exposure to fires for a short period of time. This will protect paper records, held in the cabinets, from any minor fires that break out on the building premises.

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.

Fire Alarm System

The Trust will maintain a fire alarm system at its premises to alert individuals of potential fires and so the necessary fire protocols can be followed.

Systems Security

As well as physical security the Trust also protects against hazards to its IT network and electronic systems. It is recognised that the loss of, or damage to, IT systems could affect the Trust's ability to operate and could potentially endanger the lives of its Pupils.

The Trust will implement the following systems security controls in order to mitigate risks to electronic systems:

Software Download Restrictions

All schools within the Trust use a Firewall that features anti-malware protection, HTTPS inspection, anonymous proxy detection & blocking, intrusion detection & prevention and web-filtering.

Phishing Emails

In order to avoid the Trust's computer systems from being compromised through phishing emails, employees are encouraged not to click on links that have been sent to them in emails when the source of that email is unverified. Employees will also take care when clicking on links from trusted sources in case those email accounts have been compromised. Employees will check with the Trust's ICT Team if they are unsure about the validity of an email.

Firewalls and Anti-Virus Software

The Trust will ensure that the firewalls and anti-virus software is installed on electronic devices and routers. The Trust will update the firewalls and anti-virus software when updates are made available and when advised to do so by the SECAT ICT Team. The Trust will review its firewalls and anti-virus software on an annual basis and decide if they are still fit for purpose.

Shared Drives

The Trust maintains a shared drive on its servers. Whilst employees are encouraged not to store personal data on the shared drive it is recognised that on occasion there will be a genuine business requirement to do so.

The shared drive will have restricted areas that only authorised employees can access. For example a HR folder in the shared drive will only be accessible to employees responsible for HR matters. The Headteacher, who may delegate to a member of their team, will be responsible for giving shared drive access rights to employees. Shared drives will still be subject to the school's retention schedule.

Communications Security

The transmission of personal data is a key business need and, when operated securely is a benefit to the Trust and pupils alike. However, data transmission is extremely susceptible to unauthorised and/or malicious loss or corruption. The Trust has implemented the following transmission security controls to mitigate these risks:

Sending Personal Data by post

When sending personal data, excluding special category data, by post, the Trust will use Royal Mail's standard postal service. Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject.

Sending Special Category Data by post

When sending special category data by post the Trust will use Royal Mail's 1st Class Recorded postal service. Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject. If the envelope contains information that is thought to be particularly sensitive then employees are advised to have the envelope double checked by a colleague.

Sending Personal Data and Special Category Data by email

The Trust will only send personal data and special category data by email if using a secure email transmission portal or if the data is password protected with the password sent in a separate email or communicated in person.

Employees will always double check the recipient's email address to ensure that the email is being sent to the intended individual(s). Use of autocomplete should be strongly discouraged.

Exceptional Circumstances

In exceptional circumstances the schools may wish to hand deliver, or use a direct courier, to ensure safe transmission of personal data. This could be because the personal data is so sensitive that the usual transmission methods would not be considered secure, or because the volume of the data that needs to be transmitted is too big for usual transmission methods.

Using the BCC function

When sending emails to a large number of recipients, such as a mail shot, or when it would not be appropriate for recipients to know each other's email addresses, then Trust employees must utilise the Blind Copy (BCC) function.

Surveillance Security

The Trust may or may not operate CCTV at its premises.

Due to the sensitivity of information that could be collected as a result of this operation, the Trust has a separate policy which governs the use of CCTV. This policy has been written in accordance with the ICO's Surveillance Code of Practice.

Remote Working

It is understood that on some occasion employees of the Trust will need to work at home or away from the school premises. If this is the case then the employees will adhere to the following controls:

Lockable Storage

If employees are working at home they will ensure that they have lockable storage to keep personal data and Trust equipment safe from loss or theft. If the employee does not have access to lockable storage then they may apply to the school for assistance in purchasing such storage, at the discretion of the Headteacher/COO/CEO.

Employees must not keep personal data or Trust equipment unsupervised at home for extended periods of time (for example when the employee goes on holiday).

Employees must not keep personal data or Trust equipment in cars if unsupervised, unless in a locked boot.

Private Working Area

Employees 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).

Employees should also take care to ensure that other household members do not have access to personal data.

Trusted Wi-Fi Connections

Employees will only connect their 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 employees should ensure that they have appropriate anti-virus software and firewalls installed to safeguard against malicious intrusion. If in doubt employees should seek assistance from SECAT ICT Team.

Encrypted Devices and Email Accounts

Employees will not use personal devices for storing data. This is because personal devices do not possess the same level of security as a Trust issued device.

Employees will not use personal email accounts to access or transmit personal data. Employees must only use school issued, or Trust authorised, email accounts.

Data Removal and Return

Employees will only take personal data away from the school premises if this is required for a genuine business need. Employees will take care to limit the amount of data taken away from the premises.

Employees will ensure that all data is returned to the school premises either for re-filing or for safe destruction. Employees will not destroy data away from the premises as safe destruction cannot be guaranteed.