



# Elmlea Schools' Trust

## Information Security Policy

### Document History Record of recent Policy changes

Date	Version	Author/Owner	Change	Origin of Change e.g. TU request, change in legislation
January 2020	1.0	Clare Sanders		Appointed DPO i-West – recommended policy
January 2021	2.0	Andrea Bizley	More information on areas needing specific information security, and more detail on roles and responsibilities	Annual DPO Update
November 2022	3.0	Andrea Bizley	Minor updates	Annual DPO Update
November 2023	4.0	Andrea Bizley	Updates shown in yellow	Annual DPO update

Data Protection Officer (DPO)	<a href="mailto:i-west@bathnes.gov.uk">i-west@bathnes.gov.uk</a> Organisation: One West (part of Bath and North East Somerset Council) <a href="http://www.onewest.co.uk">www.onewest.co.uk</a>
Trusts' Data Processing Lead	Director of Finance and Operations

Trustee 'Committee	Audit and Risk Committee
Policy Adopted	November 2023
Review cycle	Annually and when the following circumstances occur: Change of Data Protection Officer, Change of Legislation
Review date	Autumn 2024

## Contents

1. Introduction.....	3
2. Scope.....	3
3. Aim.....	3
4. Roles and Responsibilities.....	4
5. Areas That Require Specific Adoption of Information Security.....	7
6. Associated Policy and Guidance .....	11
7. Approval .....	<b>Error! Bookmark not defined.</b>
<a href="#"><u>Appendix 1 – Information Security Procedures.....</u></a>	<a href="#"><u>11</u></a>
<a href="#"><u>Appendix 2 – Setting up an Email Sending Delay.....</u></a>	<a href="#"><u>13</u></a>
<a href="#"><u>Appendix 3 – Securing an email in transit.....</u></a>	<a href="#"><u>14</u></a>



## Information Security Policy

### 1. Introduction

Elmlea Schools' Trust (EST) is responsible for the control of a number of individuals' Personal Data (PD) including staff, governors, pupils, clients, and a number of other individuals who interact with EST. In addition to PD, information that may be considered of a sensitive nature will include financial records, planning and management forecasts, and risk assessments, which also require appropriate security applications to be made and are included within the scope of this policy.

The Information Security Policy (ISP) is designed to inform employees of the appropriate principles and methods to create, store, secure and, dispose of information in all formats to ensure security is of a consistently high standard. Compliance with this Policy provides management, staff, and associated individuals with:

- Assurance that information is being managed securely in a consistent and effective way.
- Assurance that EST is able to provide a trusted environment in which to handle information as part of its activities.
- Clarity regarding the individual responsibilities for Information Security.
- Demonstration of best practice.
- Assurance that information may only be accessed by those authorised to have access.

### 2. Scope

This policy applies to all employees of EST including contract, agency and temporary staff, Trustees, Governors, volunteers and employees of partner organisations working with or for EST.

The ISP can be used by employees who use data as part of their day to day business, those who manage and administer data and by those responsible for the management of data storage systems.

### 3. Aim

The ISP aims to ensure that all employees are aware of the following principles of the 'CIA Triad' (confidentiality, integrity, and availability) when dealing with information and use the principles from their day-to-day handling of information up to the development and adoption of new ways and systems designed for handling information. These principles will also help EST comply with Article 32 of the GDPR which refers to adequate organisational and technical security;

**Confidentiality** - Information is not made available or disclosed to unauthorised individuals, entities, or processes.



***Integrity*** - Maintain the accuracy and completeness of data over its lifecycle.

***Availability*** - Information must be available when needed and appropriate means of access or disclosure must be understood.

In addition to the protection and maintenance of the confidentiality, integrity, and access of data this policy will support EST to meet the following:

- Manage the risk of security exposure or compromise.
- Assure a secure and stable information technology (IT) environment.
- Identify and respond to events involving information asset misuse, loss or unauthorised disclosure.
- Monitor systems for anomalies that might indicate compromise: and
- Promote and increase the awareness of information security.

Adoption of this concept will reduce the risk of harm to individuals, reduce the vulnerability of the organisation, and the likelihood of financial penalties that may be given by supervisory authorities such as the Information Commissioner's Office (ICO).

#### **4. Roles and Responsibilities**

##### ***Information Security Lead***

Accountability for Information Security rests with the Information Security Lead who is the Director of Finance and Operations. The Information Security Lead may discharge this function to the Business manager or the Office Manager to carry out the activities of Information Security.

Such activities may include.

- Evaluating and accepting risk on behalf of the school
- Identifying information security responsibilities and goals and integrating them into relevant processes.
- Supporting the consistent implementation of information security related policies and processes.
- Supporting security through the clear direction and demonstrated commitment of appropriate resources.
- Promoting awareness of information security best practices through the regular dissemination of relevant material such as that provided by the Data Protection Officer (DPO).
- Implementing the process for determining information classification and categorisation, based on recommended practices, and legal and regulatory requirements, and to determine the appropriate levels of protection for information.
- Implementing the process for information asset identification and recording them in the Record of Processing Activities (RoPA) as well as handling, use, transmission, and disposal based on the information classification and categorisation.
- Determining who will be assigned to serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data.



- Participating in the response to security incidents
- Complying with notification requirements in the event of a breach of personal data
- Adhering to specific legal and regulatory requirements related to information security.
- Communicating legal and regulatory requirements to the designated security representative (e.g., Information Security Officer ISO), specifically article 32 of the UK GDPR (security of processing)
- Communicating requirements of this policy and the associated standards, including the consequences of non-compliance, to the workforce and third parties, and addressing adherence in third party agreements.
- Development of localised guidelines for the use of specific systems, training plans, threat awareness and updates, spot checking and auditing.

Governance of Information Security may be formalised to include a regular review and working group to identify business requirements and how they impact existing information use and future use.

### ***Data Protection Officer (DPO)***

The DPO, i-West, is responsible for monitoring the organisation's compliance with Data Protection legislation. This is completed by the following means: an annual assurance review; breach and security incident monitoring; and review and providing sufficient guidance to the Information Security Lead for them to carry out their task where PD may be processed.

The DPO will support the organisation in the event of any breach of information where it relates to personal data.

### ***Senior leaders***

Senior leaders are primarily responsible for ensuring the security of their physical environments where information is processed or stored. They are also responsible for the following:

- Ensuring all employees within their area of work are aware of the relevant policies applicable to their role i.e. Acceptable Use Policy, Confidentiality agreements, Bring Your Own Device (BYOD) guidelines and e-Safety.
- Determining and controlling the access levels of employees and relaying that information, including when access must be removed, to the DFO individual responsible for the control of electronic access.
- The control of passwords, keys, combination lock numbers or any other physical form of access control within their area of work.
- Ensuring that employees have taken part in the relevant and adequate training in a timely manner.
- Making employees aware of security breaches or threats and translating points learnt from such incidents into working practices.

### ***Director of Finance and Operations (DFO)***



The DFO, being responsible for management of IT (whether on-site or through a third-party contract), must ensure that all network, mobile devices, and removable media assets are securely controlled and managed. This includes maintaining appropriate storage facilities, producing and reviewing guidance regarding the safe storage and use of assets, user access agreements and user access control, such as the removal of users when informed to do so by managers, or under exceptional circumstance. The DFO may delegate the day to day management of assets to the Office manager who will work with the Site manager to ensure all assets are correctly logged on Parago.

The maintenance of software in use by the organisation. This includes software patching routines, application or alterations or the removal of software considered to be vulnerable, the assessment of such levels of vulnerability, and the notification to all relevant staff of existing threats, emergent threats, and appropriate safe use. This information may be provided to managers in support of their responsibilities for awareness.

The development and implementation of new technologies to build safe and secure systems. The direction of this responsibility should be agreed with the Information Security Lead.

### ***Information Owners/Responsible Persons***

The approach to the use of data will determine who Information Owners are. In general, the ownership or responsibility will fall to the relevant manager, or person who retains and uses the information within their workspace, for example the Office Manager will own the data used within the School/Trust office, including centralised pupil information; the Designated Safeguarding Lead (DSL) will own Safeguarding Information; and individual teachers will own class lists and pupil information where it is not held on the Pupil Information Management System.

It is good practice to record the relevant owner or responsible person so that any issue regarding the use, management or breaches of that information may be brought to their and the DPO's attention. This is referred to as an Information Asset List, however it may be incorporated into the Record of Processing Activities used for Data Protection purposes.

Information Owners will be responsible for managing the accuracy and security of their data. This will mean that their relationship with their peers and managers, where applicable, is key to ensuring the CIA Triad is observed.

Owners will also need to discuss with the Information Security Lead and DPO the implications of using third parties to process information or when sharing information. Where this includes Personal data or other sensitive information, appropriate agreements must be in place.



### ***All Employees and External Individuals***

Everyone is responsible for Information Security and should be aware of and understand the requirements of on them in line with this Policy and any associated guidance, such as e-Safety, Acceptable Use, confidentiality agreements and the conditions of use of any device issued by EST.

The key points for all employees to remember are;

- What information they are using, and how it should be handled, stored, or destroyed to protect confidentiality, integrity and availability of information entrusted to them.
- Protecting information and resources from unauthorised use or disclosure
- Protecting personal, private, sensitive information from unauthorised use or disclosure
- What procedures, standards and agreements exist for the sharing of information with others.
- How to report breaches.
- Their responsibility for raising their concerns with their manager, the relevant Information Owner, DPO or Information Security Lead.

Individuals who may work in EST's Schools with access to information but not be an employee, such as IT technicians, auditors or external agencies, should be able to demonstrate their organisation's Information Security approach or have an appropriate confidentiality statement within their work description.

They should be made aware of what they should do if they inadvertently access information that they should not have done or discover a breach. This may be as simple as letting them know to contact the person who is responsible for them or making them aware of who the relevant manager is that they can report to.

## **5. Areas That Require Specific Adoption of Information Security**

### ***Contracts of Employment***

Staff suitability must be assessed at all points of employment, in line with safer recruitment policies and guidance, and all employee contracts must contain reference to confidentiality. Information in the form of the Acceptable Use Policy, Data Protection Policy or specific confidentiality guidance must be provided to employees at the appropriate time.

### ***Control of Information Access***

Information shall be restricted to only those who have an acceptable business reason to access such information. Information Owners/Responsible Persons must be consulted before access is granted or an



appropriate process of access must be in place. Passwords or emergency access without authorisation may only be made in exceptional circumstances and the decision to do so must be relayed to the relevant Information Owner, Manager, or the Information Security Lead at the earliest possible point.

#### Staff owned Devices

- Staff must not use their own devices to take images of young people. Only school equipment may be used, and images must be deleted as soon as they are no longer required, saved securely on the school system and deleted in accordance with the retention policy.
- Passcodes or PINS must be set on personal devices to aid security and where possible encryption applied to the device.
- Users are expected to act responsibly, safely, and respectfully in line with current acceptable use agreements.
- Users must log out of school programmes and applications when they are not in use
- The device must have the latest updates applied.
- Passwords must not be saved, for example to the browser history.
- Users must not download data locally to the device (e.g., email attachments)

#### ***Computer Access Controls***

Access to computer systems must be managed by the DFO who discharges this responsibility to the Office manager and Computeam. This may be by active directory or, in the case of portable devices, by providing a temporary password. There must be a form of system monitoring that can be used to determine who accessed which device and at what time, at a basic level this may be using Active Directory, Event Viewer or a more complex User activity Monitor (UAM) software. The fundamentals of password security are required to ensure that passwords are not shared which would result in misidentification with the exception of the point regarding emergency access in the previous paragraph.

#### ***Application Access Controls***

Specific applications must be administered effectively by either IT or the responsible person for any third-party application, such as Tapestry, Seesaw etc. This is particularly relevant for the Pupil Management System; however, it applies to all other applications where it has been deemed that access controls are required. When adopting a new application, a proper assessment of access controls must be made and, if necessary, locally produced guidelines regarding its use should be made. This may be covered as part of a Data Protection Impact Assessment. Where Personal data is being processed, the project lead must consider whether a Data Protection Impact Assessment (DPIA) is required (for high-risk processing) at the outset. The DPO must be consulted about any DPIAs completed.





## ***Equipment Security***

Information may be stored in physical containers such as filing cabinets, drawers, safes and storage rooms. It will in most cases be retained electronically, however the principles of security are the same.

Any area where information is stored must be secured in a manner appropriate to the type and sensitivity of information stored within, for example sensitive financial records, safeguarding records and HR records must be secured by lock, or if stored electronically on a secure section of the computer network isolated by specific permissions. General lists and necessary contact details should be stored out of sight in line with a clear desk routine, or, if stored electronically, may be stored in a general open section of the computer network. Information Owners must make an assessment of the level of security required and where necessary consult with the Information Security Lead and Business manager. In cases where highly sensitive information is stored electronically, it should be encrypted wherever possible.

## ***Computer Network Procedures***

The arrangement and control of the computer network should be documented and must not remain with a single person. The reliance upon a sole individual's understanding of the system can undermine the principle of availability, if they leave or are unavailable, due to the potential loss of access, and may lead to loss of data if a full understanding of the type and location of data is not retained.

## ***Information Security Breaches and Reporting***

Any breaches of information security must be reported to the DFO and, where it involves the inappropriate access via hacking, malicious attack, lack of security around an electronic system, loss of physical device or any other similar situation, Computeam must be informed.

In instances where there is the potential breach of personal data the DPO must also be informed at the earliest possible point (see EST's Data Breach Policy).

The confidentiality or security of information that has been breached which was held in a physical format, i.e. paper record, application form or folder, does not need to be reported to IT in most circumstances, however the Information Security Lead must still be informed.

## ***Protection from Malicious Software***

EST and its IT providers shall use software protection to detect and deny intrusion, email filtering and if possible, adopt measures such as SPF, DKIM and DMARC (to stop the organisation's email addresses getting spoofed). Users should not be able to install software on the Organisation's network without prior approval or introduce malicious software via other routes, i.e. the use of unmanaged USB devices.



The Trust should have a documented process for Cyber Security, seek formal accreditation of IT processes, or adopt standards that equate to accreditation.

### ***Removable Media***

Any removable media should be supplied and managed by the Organisation and controlled effectively by the use of an asset register. The Register should contain who has which device, when it was issued and who issued it. Frequent auditing of issued devices should take place in order to identify any unknown losses. USB port access should, if possible, be restricted either fully or to a select computer, user, or managed device.

Any external information device that someone wishes to use should be submitted to their manager and IT for approval prior to use. Where PD or information of a sensitive nature may be stored, encryption must be applied to removable media devices.

Encryption should be used as standard on removable devices, this may be in the form of a partitioned and password protected section of a USB Drive or a full device encryption on a standalone device.

### ***Monitoring System Access and Use***

Systems should, where possible, be adopted that can provide an auditable trail of access, this is considerably more important as the type and sensitivity of the information being accessed

increases. In terms of physical records, this may be limitation to a single or small number of individuals or a signing in and out form, this may be particularly applicable to records that contain special categories of personal data.

Electronic systems will, in many cases, have event record logs, however the Organisation must ensure that they understand how this function works and how it may be used when required, or, if it is inadequate, be able to work with their IT provider to apply any additional software as necessary.

The organisation must make it clear to employees that information contained on the Organisation's system is subject to access and monitoring and that, except in exceptional or agreed circumstances, should not be used for personal reasons by employees. The limitations of this may be defined in the Acceptable Use Policy, contract terms or specific guidelines created for this purpose.

### ***Accreditation and Assessment of Systems***

The DFO must be assured that new systems, be they physical or electronic, are adequately assessed by the relevant manager, or responsible person. Such assessment may not need to be formally documented but



demonstration of the assessment must be recorded appropriately. Recognised accreditation will provide a significant level of assurance; however, it must be taken into account with the intended way of using any application.

### ***System Control Change***

Any change made to any system must be confirmed with the Information Owners and, where any conflict arises, must be referred to the Information Security Lead. Access abilities to alter any system parameters should adhere to the Principle of Least Privilege.

### ***Business Continuity and Disaster Recovery Plans***

The DFO is responsible for ensuring that, in the event of any catastrophic failure of a system, there is adequate capability for the continuation of the use of information in line with the CIA Triad. Any system which is deemed to be critical to the organisation should be included within a Business Continuity Plan, this may include the Pupil Management System, access to financial resources or safeguarding information.

Cyber Incident Response Plans (CIRP) will be adopted and tested and also form part of the Trust's Business Continuity plan.

### ***Training and Awareness***


Information security may not be considered a separate training topic in its own right; however, the CIA Triad should underpin any training in relation to the processing of data. This will include system use and operation, data protection training, safeguarding, and procurement training.

## **6. Associated Policy and Guidance**

- Data Protection Policy
- Data Breach Policy
- Staff Acceptable Use Policy
- Online Safety / E-Safety Policy

## Appendix 1 – Information Security Procedures

All users must protect personal data:

- 1) By **Locking screens** when away from their desks (using Windows Button  +L)
- 2) By **disposing of information and equipment** in an appropriate manner:
  - a. Equipment – via the organisation’s accredited provider
  - b. Paper – using either a cross cut shredder or the organisation’s accredited provider which may be facilitated by Confidential Waste receptacles.
- 3) By ensuring **special categories of personal data**<sup>1</sup> is given extra security, and at a minimum is locked away when not in use (<sup>1</sup> *race/ethnicity, religion, genetics, health, photos, sexual orientation, trade union, political opinions*)
- 4) By using encryption when **processing personal data offsite** e.g. working at home (either on an encrypted device or an encrypted USB stick owned by the organisation). For encrypted sticks users must
  - a. ensure the information is uploaded back to the organisation’s network as soon as possible, and;
  - b. only process the data on the stick and not process or save the data outside of the stick (e.g. locally to the device).
- 5) When processing data on an unmanaged (**personal device**) users must ensure:
  - a. The device is protected by PIN, Password or fingerprint, and ideally encrypted
  - b. That the organisation’s systems (e.g. Webmail) are not left logged in
  - c. That attachments are not opened (and downloaded), unless in an emergency where measures are to be taken to delete the information after use
- 6) **Data taken offsite must be protected at all times**, as well as the above, users must:
  - a. Keep information and equipment on their person at all times (e.g. when stopping off on the way home)
  - b. Be held in an appropriate receptacle (e.g. bag) to reduce the risk of opportunistic theft
  - c. Not store leave the information and equipment in a vehicle when not in use
  - d. Consider whether data minimisation could be used. For example:
    - i. Not making the information personally identifiable, by using pseudonymisation (e.g. Unique reference or initials)
    - ii. Using a code system or colour code system to identify key indicators (e.g. allergies)
    - iii. Not having the organisation logo on any hardcopy documents
    - iv. Using encryption to protect the data (e.g. encrypted device rather than hard copies)
- 7) **By ensuring care is taken with emails**, by applying the following:
  - a. Was I expecting this email?
  - b. Does it look and feel right?
  - c. Can I check (by other trusted means) that the email is legitimate?
  - d. Not clicking any links or opening any attachment with validating them
  - e. Using blind copy (BCC) when emailing more than one external user
  - f. Double checking the email address when sending emails



- g. Encrypting personal data to external addresses ([See Appendix 3](#))
  - h. A two-minute email delay rule is in place on all emails sent, this provides a safety net where all emails sent are held in Outbox for two minutes before delivery allowing the user to edit/delete ([See Appendix 2](#))
- 8) By ensuring any **information disclosed verbally** is
- a. Validated – the person calling/present is known to have the need to know
  - b. Documented – a summary of what was disclosed and filed
- 9) By ensuring any **information sent via post has the address double checked** – where possible copy and paste from a system and is marked Private & Confidential

## Appendix 2 – Setting up an email delay (in Outlook 2013)

This can either be setup by a user or, with the aid of the organisation's IT Team, can be setup corporately.

1. Click the **File** tab.
2. Click **Manage Rules and Alerts**.
3. Click **New Rule**.
4. In the **Step 1: Select a template** box, under **Start from a Blank Rule**, click **Apply rule on messages I send**, and then click **Next**.
5. In the **Step 1: Select condition(s)** list, click **Next**.  
If you do not select any check boxes, a confirmation dialog box appears. If you click **Yes**, the rule that you are creating is applied to all messages that you send.
6. In the **Step 1: Select action(s)** list, select the **defer delivery by a number of minutes** check box.
7. In the **Step 2: Edit the rule description (click an underlined value)** box, click the underlined phrase **a number of** and enter the number of minutes for which you want the messages to be held before sending.  
Delivery can be delayed up to 120 minutes (suggested 1 or 2 minutes).
8. Click **OK**, and then click **Next**.
9. Select the check boxes for any exceptions that you want.
10. Click **Next**.
11. In the **Step 1: Specify a name for this rule** box, type a name for the rule.
12. Select the **Turn on this rule** check box.
13. Click **Finish**.

After you click **Send**, each message remains in the **Outbox** folder for the time that you specified.



## Appendix 3 – Securing an email in transit

The three main risks associated with email are:

- 1) Emails are intercepted in transit
- 2) Emails are sent to the wrong recipient
- 3) Email addresses are disclosed to those without the need to know

This process covers risk (1) and enables the secure exchange of information over email (in the absence of a secure email portal).

- 1) Document the information in an MS Office document
- 2) Ensure that this is not the source/primary document – if it is then create a copy.  
*Do not encrypt the source document – if you do, and forget the password you are unlikely to be able to gain access to the information again!*
- 3) Have the document open, and then click
  - a. File
  - b. Protect Document
  - c. Encrypt with Password
  - d. Create a strong password (minimum of 8 characters) – you could use a password generator <https://passwordsgenerator.net/> or pre-agree one with the recipient
  - e. Apply this password to the document
  - f. Save
- 4) Attach the secured document to an email and send it to the recipient
- 5) Communicate the password by other trusted means e.g. Phone call, or message. Before telling them, the password ensure you:
  - a. Are communicating with the correct person; and
  - b. Confirm that they have received the email*It should be noted that encrypted attachments are sometimes blocked by email gateways as they cannot inspect the contents*