Pickwick Academy Trust

Information Security Policy

Policy Group:	**Admin & Data**
Policy Ref:	**ADD/05**
Responsible Reviewing Officer and Job Title:	**Emma Oldale, CFOO i-West, DPO**
Date Written:	**November 2025**
Date Approved by the Board:	**November 2025**
Date of Next Review:	**November 2027 unless a newer template or further guidance is issued by our DPO**

Contents

1. Introduction

a. Pickwick Academy Trust is responsible for the control of a number of individuals' Personal Data including staff, trustees ,governors, pupils, and a number of other individuals who interact with Pickwick Academy Trust. In addition to Personal Data, 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.

b. The Information Security Policy 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 Pickwick Academy Trust 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. Purpose and Scope

a. The Information Security Policy aims to ensure that all employees are aware of the following principles of the CIA Triad below (confidentiality, integrity, and availability) when dealing with information and use the principles from their day to day handling of information to inform the development and adoption of new ways and systems designed for handling information. These principles will also help Pickwick Academy Trust 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.

b. In addition to the protection and maintenance of the confidentiality, integrity, and access of data this policy will support Pickwick Academy Trust 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.

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

d. This policy applies to all employees of Pickwick Academy Trust including contract, agency and temporary staff, Trustees, Governors, volunteers and employees of partner trusts working with or for Pickwick Academy Trust.

e. This policy 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. Definitions

Personal data - Any combination of data items which could identify a living person and provide specific information about them, their families or circumstances. The term covers both facts and opinions about an individual. Pickwick Academy Trust may process a wide range of personal data of staff (including governors and volunteers) pupils, their parents or guardians as part of its operation. A non-exhaustive list of examples of the types of personal data that we process may be found in our Privacy Notices.

This personal data may include (but is not limited to):

- Names and addresses (including email addresses)
- Bank details
- Academic data e.g. class lists, pupil progress records, reports, disciplinary actions, admissions and attendance records
- References
- Employment history
- Taxation and national insurance records
- Appraisal records

Special category personal data – Formally known as 'sensitive personal data' special category data is information which is more sensitive and so needs more protection. Categories for a living individual are:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns, voice biometrics), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation

Data Breach - The most common type of data breach is the accidental or unlawful *loss, alteration, destruction, disclosure of or access to* personal data, for example sending an email to the wrong recipient, losing a file containing personal data, or sharing passwords enabling someone else to access your account. However, you should consider any failing of one of the Data Protection Principles (Article 5 of GDPR) as a GDPR breach, this could include examples such as not having the necessary paperwork in place, not providing the data subject with clear privacy information, retaining personal data for longer than is necessary or processing personal data without an identified lawful basis (Article 6 of GDPR).

Near Miss - an unexpected event where someone could have been hurt or information could have been lost, but it wasn't. In the context of GDPR, an example could be leaving pupil records unsecured in a space where visitors/ volunteers are present.

4. Responsibilities and Accountabilities

a. The Trust Board

The Trust Board has overall responsibility for ensuring that Pickwick Academy Trust complies with all relevant data protection obligations and is responsible for reviewing and approving this policy.

b. The CEO

The CEO is responsible for the broadcast of this policy across the trust and for its promulgation through the CFOO, Directors of Education, Headteachers and central team Heads of Department.

c. The CFOO

Accountability for Information Security rests with the Information Security Lead who is the CFOO. The CFOO discharges elements of this function to the Trust Chief Technical Officer, the Head of Governance and Compliance, or another responsible individual to carry out the activities of Information Security.

Such activities may include:

    - Evaluating and accepting risk on behalf of the Trust.
- Development of trust policies and Data Processing Impact Assessments for the use of specific systems, training plans, threat awareness and updates, spot checking and auditing.
    - Supporting the consistent implementation of information security related policies and processes.
    - Supporting security through 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 information asset identification and ensuring that they are recorded in the trust Record of Processing Activities as well as the handling, use, transmission, and disposal based on information classification and categorisation.
- Ensuing compliance with notification requirements in the event of a breach of personal data.
- Participating in the response to security incidents
    - Adhering to specific legal and regulatory requirements related to information security.
-

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.

The CFOO, being responsible for management of IT, must ensure that all Laptops,Desktops, Network devices, mobile devices, and removable media assets are securely controlled and managed. For Pickwick Academy Trust, these elements are discharged to our external IT support company. This includes:

- The maintenance of 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 maintenance of software in use by the trust. 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.

d. Chief Technical Officer

The Chief Technical Officer, in conjunction with the IT support company, is responsible for supporting the CFOO with the above activities, including the reporting of any concerns. Jack Miles, Head of Primary EdTech Solutions at Oakford Technology, performs this function.

e. Data Protection Officer (DPO)

The DPO, One West, is responsible for monitoring the trust'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 CFOO for them to carry out their task where Personal Data may be processed.

f. Headteachers/ Central Team Department Heads

Heads are primarily responsible for ensuring the security of the systems that hold data and the physical environment where information is processed or stored (filing cabinets, cupboards etc). They are also responsible for the following:

- Ensuring all employees within their school are aware of the relevant polices applicable to their role i.e. Online Safety Policy and Acceptable Use Agreements.
- Determining and controlling the access levels of employees, as determined by the completion of Appendix 3 of the trust Induction Policy (IT Network and Software Access) and relaying that information, including when access must be removed, to the individuals responsible for the control of electronic access. In respect of the trust this will be the external IT support provider.
- 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 data protection training annually.
- Making employees aware of security breaches or threats and translating points learnt from such incidents into working practices.
- Ensuring that they are aware of the information owners for the various departments in their schools.

g. 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 Admin Officer will own the data used within the School/Trust office, including centralised pupil information the Designated SafeguardingLead (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.

The trust will consider additional good practice to record the relevant owner or responsible person in key areas so that any issue regarding the use, management or breach 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 CFOO, CTO 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.

h. All Employees and External Individuals

Everyone is responsible for Information Security and should be aware of, understand and abide by the requirements of them in line with this Policy and any associated guidance, such as the trust Online Safety policy and associated Acceptable Use Agreements., and the conditions of use of any device issued by Pickwick Academy Trust.

The key points for all employees to remember are;

- What information they are using, and how it should be handled, stored, or destroyed to prevent unauthorised use or disclosure, especially in respect of personal, private and sensitive data
- What security controls are necessary and in place to protect the confidentiality, integrity and availability of information entrusted to employees from unauthorised use or disclosure
- What policies and procedures, exist for the sharing of information with others
- How to report breaches and near misses.
- Their responsibility for raising their concerns with their manager, the relevant Information Owner, DPO or CFOO.

Individuals who may work in Pickwick Academy Trust's Schools/ central team with access to information but not be an employee, such as IT technicians, auditors or external agencies, should be able to demonstrate

their trust'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

a. 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 Online Safety Policy incorporating Acceptable Use Agreements, Data Protection Policy or specific confidentiality guidance must be provided to employees at the appropriate time.

b. Control of Information Access

Information shall be restricted to only those who have an acceptable business reason to access such information. Headteachers, or the CFOO for the central team, 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 very exceptional circumstances and the decision to do so must be relayed to the Headteacher or CFOO at the earliest possible point.

c. Staff Owned Devices

Any use of personal devices must be done in accordance with the requirements of the trust Online Safety Policy.

d. Computer Access Controls

Access to computer systems must be managed by the trust IT support providers on behalf of the trust. 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 (currently in place) or a more complex User Activity Monitor (UAM) software may be considered in the future. 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.

e. Application Access Controls

Specific applications must be administered effectively by either the trust IT support providers 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.
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 Data Protection Officer (DPO) must be consulted about any DPIAs completed.

f. 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 CFOO, CTO or DPO. In cases where highly sensitive information is stored electronically, consideration should be given to additional encryption where possible.

g. Computer Network Procedures

The arrangement and control of the computer network is the responsibility of and should be documented by the trust IT support provider. It 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.

h. Information Security Breaches and Reporting

Any breaches of information security must be reported to the CFOO 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, the trust IT Support providers 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 Pickwick Academy Trust'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 CFOO must still be informed.

i. Protection from Malicious Software

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

The Trust has a documented process for Cyber Security, may seek formal accreditation of IT processes by working to achieve the Cyber Essentials Accreditation, and may adopt standards that equate to accreditation.

Use of antivirus is deployed to all laptops, desktops and servers to ensure detection and protection against malicious software. The antivirus tool used will detect malicious activity across devices, network, email and websites. Alerts are generated in the event of detection and IT support will provide assistance to remediate. Regular scanning is performed to ensure there is no persistent threat to devices.

j. Removable Media

Removeable Media (for example USB sticks) are not permitted to be used on the trust IT network. This is enforced through remote policy by our trust IT support providers.

k. Monitoring System Access and Use

Systems will, where possible, be adopted that can provide an auditable trail of access, this is considerably more important as the type and sensitivity or the information being accessed increases. In terms of physical records, this maybe limited 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 trust will 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 support provider to apply any additional software as necessary.

Information contained on the trust's system is subject to access and monitoring and , except in highly exceptional or agreed circumstances, should not be used for personal reasons by employees. Please see the trust Online Safety Policy and Acceptable Use Agreements for more information.

l. Accreditation and Assessment of Systems

The CFOO must be assured that new systems, be they physical or electronic, are adequately assessed by the relevant Headteacher with support from the trust IT support provider. 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.

m. 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 CFOO or CTO. Access abilities to alter any system parameters should adhere to the Principle of Least Privilege.

m. Business Continuity and Disaster Recovery Plans

The CFOO, with support from the CTO 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 trust should be included within the trust Cyber Security Response Plan ,this may include the Pupil Management System, access to financial resources or safeguarding information.

n. 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. Legislation and Guidance

This policy takes into account the following:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act (DPA) 2018.
- The Protection of Freedoms Act 2012
- Guidance published by the Information Commissioner's Office
- Protection of biometric information of children in schools and colleges - DfE July 2022
  Information Sharing – Advice for Practitioners – DfE July 2018.

7. Links with Other Policies

This Information Security Policy is linked to the following:

- Data Protection Policy
- Records Management Policy
- Data Breach Policy
- Privacy Notices
- Safeguarding and Child Protection Policy
- Online Safety Policy and Acceptable Use Agreements
- Consent / Permissions Forms
- Admissions Form

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 trust's accredited provider – please speak to your finance manager for support
   b. Paper – using either a cross cut shredder or the trust/ schools 's accredited provider which may be facilitated by Confidential Waste receptacles.

3) By ensuring **special categories of personal data**[1] is given extra security, and at a minimum is locked away when not in use ([1] *race/ethnicity, religion, genetics, health, sex life, sexual orientation, trade union, political opinions*)
4) By using encryption when **processing personal data offsite** e.g. working at home on an encrypted trust device).
5) When processing data on an unmanaged (**personal device**) users must ensure:
    a. The device is protected by PIN, Password or fingerprint, and encrypted
    b. That the trust's systems (e.g. Webmail) are protected by multi-factor enrolment and re-authentication takes place when prompted.
    c. That attachments are not downloaded, unless in an emergency where measures are to be taken to delete the information immediately after use
6) **Data taken offsite must be protected at all times**, as well as the above, users must ensure that they do so in line with section 7:
    a. Keep information and equipment on their person at all times (in the case of Special Category Data) (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, unless low sensitivity when it must be placed in the boot of the vehicle for the shortest of times and never overnight
    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 trust 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? Does it purport to come from a co-worker but not seem genuine?
    c. Can I check (by other trusted means) that the email is legitimate? For example, hovering over any links to ensure they are genuine.
    d. Not clicking any links or opening any attachment prior to validating them
    e. Be wary of an urgent subject line
    f. Using blind copy (BCC) when emailing more than one external user
    g. Double checking the email address when sending emails
    h. Encrypting personal data to external addresses (See Appendix 3)
    i. A one or 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 one/ 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 trust'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 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 documents in order to email

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