Pickwick Academy Trust

Data Breach Policy

Policy Group:	**Admin & Data**
Policy Ref:	**ADD/07**
Responsible Reviewing Officer and Job Title:	**Emma Oldale, CFOO i-West, DPO**
Date Written:	**June 2025**
Date Approved by the Board:	**July 2025**
Date of Next Review:	**June 2026**

Contents

1. Introduction

a. Pickwick Academy Trust issues this policy to meet the requirements incumbent upon them under the Data Protection Act 2018 for the handling of personal data in its role as a data controller, such personal data is a valuable asset and needs to be suitably protected.

b. Appropriate measures are implemented to protect personal data from incidents (either deliberately or accidently) to avoid a data protection breach that could compromise security.

c. A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

2. Purpose and Scope

a. The purpose of this policy is to ensure that clear guidance on both the description and the required reporting of data breaches is provided.

b. This policy applies to all employees of Pickwick Academy Trust including contract, agency and temporary staff, trustees, governors, volunteers and employees of partner organisations working for Pickwick Academy Trust.

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
- Examination scripts and marks

Data Subject - The identified or identifiable (living) individual about whom the personal data relates or identifies and whose personal data is therefore held or processed.

Data Controller - The Data Controller is occasionally the person or more commonly the organisation with overall responsibility for the processing of personal data that organisation undertakes. They will make all the decisions about what is captured, how it's used and the purpose for it, as well as deciding what controls need to be in place.

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 but it was avoided 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 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 is responsible for the broadcast of this policy across the trust and for it's promulgation through the CFOO, Directors of Education, Headteachers and central team Heads of Department.

c. The CFOO acts with the delegated authority of the Trust Board on a day to day basis as internal Data Protection

Lead, and will liaise with the DPO. The Head of Governance and Compliance supports the CFOO in this work. In the CFOO's absence, in case of emergency, this role will be delegated to the CEO.

d. Headteachers/ are responsible for the policy's implementation in each of the Trust's schools and for ensuring that the Head of Governance and Compliance are made aware of any Data breaches. The CFOO should also be alerted in the case of any significant Data Breaches.

e. The CFOO is responsible for the implementation of this policy within the trust Central Team.

f. All staff are responsible for:

- Familiarising themselves with and complying with this policy. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes. However, staff should be aware, that a deliberate or reckless disregard of this policy could result in disciplinary action being taken;
- Taking care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse at all times. All staff should adopt the approach that they should treat the personal data of others with the same care with which they would treat their own;
- Only using computers and other devices authorised by Pickwick Academy Trust for accessing and processing personal data ensuring that they are properly "logged-off" at the end of any session in which they are using personal data; **and locking devices when they are temporarily left unattended at any point (Windows Button + L is a handy shortcut);**

- Storing, transporting and transferring data using encryption and secure password protected devices;
- Not transferring personal data offsite (unless in accordance with the guidelines in Section 7 of the trust Data Protection Policy) or to personal devices.
- Deleting data in line with this policy, the trust Records Management Policy and the retention schedule;
- Informing Pickwick Academy Trust of any changes to their personal data, such as a change of address;
- Reporting to their Headteacher, or the CFOO for those in the Pickwick Central Team, or in their absence the DPO in the following circumstances:
    - Any questions about the operation of this policy, data protection law, retaining or sharing personal data or keeping personal data secure;
    - If they have any concerns that this policy is not being followed;
    - The discovery of a data breach or near miss **(immediate action is required).**

5. Data Protection Officer (DPO)

a. The Data Protection Officer (DPO) is responsible for advising on the implementation of this policy, monitoring compliance with data protection law, providing support and developing related policies and guidelines where applicable, in amongst other data protection related functions. They will provide an annual report on compliance directly to the Board of Trustees and, where relevant, provide Pickwick Academy Trust with advice and recommendations on data protection issues.

Pickwick Academy Trust has appointed i-West as its DPO, and they can be contacted through:

Email: i-west@bathnes.gov.uk

Telephone: 01225 395959

One West
Bath and North East Somerset Council
Guildhall
High Street
Bath
BA1 5AW

Under usual circumstances the Head of Governance and Compliance will be the point of contact with the DPO, with any significant issues raised with the CFOO.

6. Data Breaches

a. For the purposes of this policy data breaches will include 'near misses', suspected and confirmed incidents.

b. An incident can include, but is not limited to:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored *(e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge)*
- Equipment failure (where this leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data)
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)

- Unauthorised disclosure of sensitive / confidential data *(e.g. login details, emails to the wrong recipient, not using BCC, post to the wrong address)*
- Website defacement
- Hacking attack
- Unforeseen circumstances (where this leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data) such as a fire or flood
- Human error
- Breaches of policy such as
    - Server Room door left open
    - Filing cabinets left unlocked
    - Temporary loss / misplacement of confidential or sensitive data or equipment on which such data is stored *(e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge)*

c. Near misses can include, but are not limited to, scenarios such as emails sent to the wrong recipient where a non-delivery report bounces back.

7. Risk Assessment and Reporting

a. The quick response to a suspected or actual data breach is key. When a security incident takes place, it should be quickly established whether a personal data breach has occurred and, if so, appropriate steps should be promptly taken to address it.

b. The focus of risk regarding breach reporting is on the potential negative consequences for individuals. On becoming aware of a breach, you should contain it and

assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

c. All parties in scope of this policy have a responsibility to report a **suspected** or **actual** data breach. If this is discovered or occurs out of hours, this should be reported as soon as practically possible to the Headteacher or CFOO, for those in the central team. This should be done through the completion of the reporting form in Appendix 1, which should be sent to the Headteacher. The Head will send a copy to the DPO and the Head of Governance and Compliance on behalf of the CFOO will liaise with the trust Data Protection Officer (One West), supported by the CFOO if required. The Head of Governance and Compliance must be copied into to all communication regarding the breach.

d. Notify the ICO (if necessary) if the personal data breach is likely to result in a risk to the rights and freedoms of an individual(s), the incident may need to be reported to the Information Commissioner's Office (ICO), no later than 72 hours after becoming aware of the breach. It is therefore crucial that you report any data breach (regardless of the severity) to your Data Protection Officer (DPO) as soon practically possible. It is especially important to report data breaches promptly where there is low staff availability and or a Bank Holiday. The DPO will advise on whether to notify the ICO, however the final decision will rest with the organisation. If a decision to report is made, then it is the Organisation's responsibility to liaise with the ICO to ensure the report is sent off.

Notify data subjects (if necessary – to be agreed with CFOO following advice from the DPO).).

e. If the breach is likely to result in a high risk to the rights and freedoms of individuals then you should promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effect of a breach. When notifying individuals, you should consider including the following:

- Outline what has occurred and apologise
- Provide name and contact details of lead officer or relevant manager for further information
- Describe any likely consequences
- Describe any measures taken or proposed to be taken to address the breach including any measures to mitigate its possible adverse effects
- Advise whether the ICO has been notified
- Record notification to the data subject in **breach log.**

8. Monitoring and compliance

a. Compliance with this policy shall be monitored through a review process. This will be agreed with the Data Protection Officer, and compliance will be reported to the board of trustees.

b. Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the organisation, in consultation with the CEO, and where appropriate, the board of trustees, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

c. All personal data breaches (and near misses) should be recorded whether ornot they have been reported to the ICO.

The breach log will include the factsof the breach, its effects and the remedial action taken. Staff should be aware, that a deliberate or reckless disregard of this policy could result in disciplinary action being taken.

d. Learning from experience

The relevant manager should, in consultation with the DPO, undertake a review of existing controls to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring. The review should consider:

- Whether policy controls are sufficient
- Whether the breach occurred due to system error or human error or both
- Whether training and awareness can be amended and/or improved (if a report to the ICO is made, they are likely to seek details of training that has been undertaken)
- Where the biggest risks are apparent and any additional mitigations
- Whether methods of transmission are secure
- If *learning from experience* should be disseminated to all staff (where possible without identifying the person responsible).

This policy will be reviewed annually, unless an incident or change to regulations or to the DPO dictates a sooner review.

9. Links with Other Policies

a. This policy should be read in conjunction with other relevant policies, including but not limited to:

- Data Protection Policy
- Information Security Policy
- Records Management Policy
- Online Safety Policy

Appendix 1 – Data Incident Reporting Form

Please send to your Headteacher (Head of Governance and Compliance for those in the central team) who should then forward to the DPO and the Head of Governance and Compliance.

1. About the incident	
Date and time of incident	
Where did the incident occur?	
Date (and time where possible) of notification to the organisation	*If there was any delay in reporting the incident, please explain why this was*
Who notified us of the incident?	
Describe the incident in as much detail as possible, including dates, what happened, when, how and why?	*Include names of staff and data subject(s). Identifying information will be anonymised for any reporting purposes.*
2. Recovery of the data	
What have you done to contain the incident?	*eg limiting the initial damage, notifying the police of theft, providing support to affected data subjects*
Please provide details of how you have recovered or attempted to recover the data, and when	*Consider collecting the lost data, rather than relying on an unintended recipient to dispose of it*
3. About the affected people (the data subjects)	
How many individuals' data has been disclosed?	

Are the affected individuals aware of the incident, and if so, what was their reaction?	
When and how were they made aware / informed?	
Have any of the affected individuals made a complaint about the incident?	
Are there any potential consequences and / or adverse effects on the individuals? What steps have been taken / planned to mitigate the effect?	
Your organisation: **Your name and contact details:**	