Potteries Educational Trust

Data Protection Policy

Potteries Educational Trust

Policy Family	Information Governance
Reference	INF-01
Responsible Manager	Chief Operating Officer
Approval Date	12 February 2026
Issue Number	5
Review Date	February 2027

Potteries Educational Trust

Change control

Date	Summary of Change	Signature
Feb 2026	Policy fully reviewed to reflect current legislation, implementation and communication arrangements updated, roles and responsibilities defined. Updated to reflect PET branding	Claire Gaygan (COO)

Aim

The Potteries Educational Trust is committed to creating an environment that is welcoming and inclusive and where everyone is treated fairly and with dignity and respect. It is a place where everyone will have the opportunity to fulfil their potential regardless of age, disability, gender reassignment and being a transsexual person, pregnancy or maternity, being married or in a civil partnership, race, religion or belief, sex, sexual orientation and socio-economic status.

The Trust needs to gather and use certain information about individuals. These individuals can include learners, parents/carers, employees, suppliers, business contacts and other people the Trust has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Trust's data protection standards and to comply with the law.

In addition, this policy will ensure that the PET fulfils its responsibilities for ensuring there is a robust framework governing how data is collected, stored and processed fairly, for deciding which types of information will be processed and the reasons for processing it.

Scope

The policy and associated operating procedures apply to The Potteries Educational Trust and its academies, collectively referred to as The Trust.

This policy applies to the PET, all employees of our Trust, whether academy based or part of the central services team along with any other people working within our academies (whether paid or unpaid), including agency/supply staff, trainee teachers, contractors and volunteers. Governors, Trustees and Members of Potteries Educational Trust are also in scope of this policy.

Policy

1. Relationship to Guidelines, Procedures, Other Policies & Legal Requirements

1.1. The Trust recognises the need to ensure compliance with the 2018 Data Protection Act (DPA), Freedom of Information Act 2000, other associated legislation, and complies with UK data protection law and follows good practice. Requests for confidentiality in respect of 'sensitive' personal data will be respected wherever possible.

1.2. This Policy meets the requirements of the:

- UK General Data Protection Regulations (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

2. Key Definitions

2.1. Data - The DPA describes how organisations, including the Trust must collect, handle and store personal information ('data').

Data is any information that the Trust and the Academies within it collects and stores about individuals or organisations. Some data is more sensitive than others and the Trust will make sure appropriate procedures are in place to ensure that particular care will be given to the secure processing and managing of this.

Sensitive data includes:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.

- Trade union membership.
- Data concerning health or sex life and sexual orientation.
- Genetic data.
- Biometric data. Data can be stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

2.2. Data Subject - A 'Data Subject' is someone whose details the Trust keeps on file. The data subject has the following rights under UK data protection law:

- To be informed.
- To have access to data stored about them (or their children).
- To rectification if there is an error on the data stored.
- To erasure if there is no longer a need for the Trust to keep their data.
- To restrict processing (for example, limit what their data is used for).
- To object to data being shared or collected.

Although data protection legislation affords these rights to individuals, in some cases the obligations the Trust has to share data with the DfE etc. override these rights (this is documented later in the policy under 'Privacy Notices')

2.3. Data Controller - The 'Data Controller' has overall responsibility for the personal data collected and processed and has a responsibility for ensuring compliance with the relevant legislation. They are able to delegate this to 'Data Processors' to act on their behalf. The Trust's Chief Operating Officer for the Trust is the 'Data Controller'.

2.4. Data Processor - A 'Data Processor' uses, collects, accesses or amends the data that the controller is authorised to collect or has already collected. It can be a member of staff, third party Company or another organisation such as the police or Local Authority (LA).

2.5. Overall Responsibility - The Trust will meet its obligations under the DPA by putting in place clear policies that focus on the key risks and in checking that control measures have been implemented and remain appropriate and effective.

3. Data Protection Awareness

In order to ensure organisational compliance, all staff and other key stakeholders (for example, trustees, governors and volunteers) will be made aware of their responsibilities under the UK data protection law as part of their induction programme, (both as a new employee/trustee/governor to the organisation or if an individual changes role within the Trust).

The Trust aims for:

- GDPR inductions to be completed 7 days after a formal induction has taken place.
- Annual data protection refresher training will take place to reinforce the importance of staff adhering to the legislation.
- A record of the professional development undertaken by the individual will be retained on their training record.
- Staff and Governors/Trustees will also be required to complete annual Cyber Security training to ensure that they are aware of cyber risks and understand the important role that they play in reducing the risk of a successful cyber-attack.
- Where appropriate local, departmental induction programmes will concentrate on specifics of their role and details on how Data Protection affects their job.
- All parties will receive notification regarding changes to policies, standards and procedures on a timely basis.

4. Individual Rights

Through the provision of clear, simple public information, the Trust will ensure that Individuals are able to exercise their legal rights in relation to Data Protection.

4.1. Right of Access - Subject Access Requests

- All Subject Access Requests will be directed by Trust staff to the appropriate Academy Data Protection Champion who will ensure that the agreed procedure is followed to establish the identity of the individual, the scope of their request, and the timely provision of a response.
- All Subject Access Requests will be recorded onto the Trust External Data Protection Service portal – SchoolPro and will follow guidance offered.
- The Trust will not charge a fee for the processing of a Subject Access Request but reserves the right to pass on the cost of providing additional or repeat copies of the same information, as well as the cost of meeting any manifestly unfounded or excessive requests.
- The Trust will aim to respond to all subject access requests within 30 days of receipt. If a request cannot be fully answered within that period, the trust will;
    - Seek to clarify the nature and scope of the request to provide the data subject with the information that they require
    - Provide as much information as possible within this timeframe, and an estimate of the time required to provide any remaining information
    - Provide regular updates to the data subject so that they are fully informed of the reasons for any delay and the likely timeframes for completion of a request
    - Provide the data subject with a detailed explanation if a subject access request is not able to be fulfilled in part or in full.

4.2. Right of Erasure (Right to be Forgotten)

- The Trust will respond to all requests for data erasure within 30 days and will confirm which categories of personal data have been erased, as well as any categories of data retained where they do not fall within the scope of this right.
- In a marketing context, where Personal Data is collected and processed for direct marketing purposes, the Trust will develop procedures that will enable the individual to object to processing at any time. Where the individual objects, the Personal Data will be erased, or if also retained for another legitimate reason, clearly annotated to prevent future use for marketing purposes.

4.3. Right of Data Portability

- The Trust will respond to all requests to provide portable data within 30 days, providing either a suitable dataset for transport, or a detailed explanation as to why the request cannot be fulfilled.

4.4. Right of Rectification and Restriction

- The Trust will use all Personal Data in accordance with the rights given to individuals under Data Protection Laws and will ensure that it allows Individuals to exercise their rights in accordance.

4.5. Automated Decision Making and Profiling

- Any Automated Decision Making or Profiling which the Trust carries out can only be done once the Trustees are confident that it complies with Data Protection Laws. If staff, therefore, wish to carry out any Automated Decision Making or

Profiling, they must inform their Data Protection champion who will advise as appropriate.

Staff must not carry out Automated Decision Making or Profiling without completing a Data Protection Impact Assessment, taking advice from the Data Protection Officer, and receiving approval from their Headteacher/Principal and CEO. The Trust does not carry out Automated Decision Making or Profiling in relation to its employees.

5. Data Mapping & Risk Mitigation

5.1. The Trust will document all of the data that it collects within a 'Data Flow Map'. This data will inventory records:

- The data held.
- What the data is used for.
- How it is collected.
- How consent is obtained.
- How the data is stored.
- What the retention period is.
- Who can access the data.
- Who is accountable for the data.
- How the data is shared.
- How the data is destroyed.

5.2. For each data type, the probability of a data breach occurring is assessed (very high, high, medium, low or very low) and actions to be taken to mitigate the risk are recorded. The map should be a live document and updated regularly.

5.3. Periodic audits will be undertaken of personal and sensitive data to ensure that only necessary data is held and that personal data is held in a secure manner. Personal data will not be released to a third party where this contravenes the DPA

6. Transparent Processing

6.1. Privacy Statements

Where the Trust collects Personal Data directly from individuals, the Trust will inform them about how the Trust uses their Personal Data through the appropriate Privacy Statement published on the Trust website.

6.2. Marketing and Consent

Where the Trust carries out any marketing, activities will be carefully planned to ensure compliance with Data Protection Law, other applicable legal and regulatory frameworks.

For Marketing activities, consisting of any advertising or marketing communication that is directed to individuals and using their personal information, the Trust will operate within a framework of consent, and maintain records within its central systems for learner records and customer relationship management.

For electronic marketing, the Trust will provide a clear and simple opt-in system for Individuals, and simple means to withdraw consent at any time.

Where information is collected face to face or by telephone, and as part of a specific marketing activity, the Trust will use a 'soft opt-in' record of consent and provide the individual with a simple opportunity to opt out on all occasions that the information is used.

6.3. Exchange of Personal Information with 3rd Parties (Data Sharing)

The details of the organisations with whom we share personal data and the legal basis for this sharing are provided in the Privacy Notices for each group of data subjects

The Trust will not disclose or sell personal information to third parties for the purposes of marketing, sales of goods and services or promotions.

The Trust will communicate policies, procedures and guidance to all staff that clearly set out when and how it is appropriate for them to share or disclose data.

Each academy will ensure appropriate data sharing agreement (DSA) are in place with any party it routinely shares personal data with or transfers large quantities of data to.

6.4. Data Quality and Use

The Trust will implement guidance and procedures that recognise the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws.

All staff who collect and record Personal Data will endeavour to ensure that the Personal Data is collected and maintained to ensure it is recorded accurately; kept up to date and limited to what is necessary in relation to the purpose for which it is collected and used.

All staff who obtain Personal Data from sources outside the Trust shall take reasonable steps to ensure that the Personal Data is recorded accurately, up to date and limited to that which is adequate, relevant and necessary in relation to the purpose for which it is collected and used.

This does not require staff to independently check the personal data obtained from outside the Trust.

Note that this does not apply to Personal Data which the Trust must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

6.5. Images and Recordings

Where the Trust collects images and/or recordings and individuals may be identified in those images, arrangements for collection, storage and disposal will be carefully considered based on the basis for processing.

The Trust will ensure that CCTV images and recordings are collected, stored and used within a secure environment, in accordance with the published procedures and codes of conduct.

The use of images and recordings created as part of the teaching, learning and assessment process will only be used to provide access and support to learners as part of their learning programme. This may include the recording of lessons and other activities, which may include images of teachers, learners and other staff. Such images and recordings will be shared with staff and learners via the agreed Digital Learning Platform(s) and therefore subject to specific, more open arrangements for security and retention.

Images and recordings of staff, created for the purposes of delivering teaching, learning and assessment through online platforms, or to create reusable teaching and learning resources, will be separately classified and subject to specific criteria for retention and re-use.

The Trust will use staff and learner photographic images solely for administrative and reference purposes only and will not use them for publicity without express permission. The use of staff images for promotional purposes will be discussed and agreed on an individual basis when appropriate. Individuals should be mindful when providing

consent for the use of photographs, that it may not be possible to remove images from printed materials once produced, and therefore any requests for erasure or to restrict processing may not apply retrospectively.

In some cases, arrangements may differ from standard procedures, for example for the security or sharing of media. In particular, the Trust will;

- Ensure that all images of learners and members of the public collected for marketing and communications purposes are supported by clear and informed consent, which may be amended or withdrawn by the individual at any time.
- The Trust will ensure that individuals are aware of the limitations of their right to restrict processing in relation to images already published in digital or paper form, and will involve individuals in the approval process for any use of their image which might have a significant public reach or impact.

7. Data Breaches

- Where there is a suspected data breach the Trust Data Breach procedure will be followed. (appendix 1)
- The COO must be informed of all suspected data breaches
- All suspected breaches will be supported by the Data Protection Champion who will liaise with their Headteacher/Principal.
- All Data breaches (including near misses) will be recorded on the Trust external Data Protection Service – SchoolPro
- Where an investigation identifies a case to be answered by one or more members of staff, this will be addressed through the Staff Disciplinary Policy.
- Where a breach occurs involving the Data Protection Champion or Data Protection Officer, the investigation will be undertaken by the COO, who will report their findings to the appropriate Head teacher/Principal

8. Roles and Responsibilities

8.1. To define roles and responsibilities for data management and protection across the Trust, providing clarity on accountability and responsibility at every level.

Accountabilities and Responsibilities for Data Protection:	
TRUST BOARD Accountable	Strategic Accountability: ○ Accountability for GDPR compliance and data protection across the Trust ○ Review and approve the Data Protection Policy annually ○ Receive reports on data breaches, compliance risks and mitigation of risks ○ Ensure robust governance framework for data management
AUDIT & RISK COMMITTEE Accountable	Oversight and Assurance: ○ Monitor effectiveness of data protection controls and risk mitigation ○ Review data protection risks on the Trust risk register quarterly ○ Monitor compliance with statutory requirements [to include retention schedules & secure disposal procedures] ○ Report findings and recommendations to Trust Board ○ Review data breach reports and lessons learned

FINANCE & RESOURCES COMMITTEE Accountable	Resource and Compliance: ○ Approve budget for data protection resources [systems, training, DPO services] ○ Review data processing contracts with third-party suppliers ○ Ensure procurement processes include data protection due diligence ○ Review cyber insurance and data breach response arrangements ○ Ensure value for money/efficiency, effectiveness and economy ○ Report financial and resource risks [related to data protection] to Trust Board
CEO Accountable Responsible	○ Overall responsibility for implementing data protection policies across the Trust ○ Champion of data protection culture throughout the Trust ○ Lead response to serious data breaches and ICO investigations ○ Report to the Trust Board on data protection compliance ○ Sign off on major data processing activities and data sharing agreements ○ Regulatory compliance (as Accounting Officer)
COO Advisory	Operational ○ Advise CEO on operational risks and mitigation [related to data protection] across the Trust ○ Day-to day operational responsibility for data protection compliance ○ Coordinate data protection activities across central and academy ○ Implement and monitor data retention and disposal schedules ○ Lead operational responses to data breaches ○ Monitor impact of data protection training programme for academies and the Trust
TRUST DATA PROTECTION OFFICER	○ Monitor Trust-wide data protection compliance and report to COO ○ Undertake data protection impact assessments for high-risk processing
DATA PROTECTION CHAMPION *[operational management academy based]*	○ Co-ordinate Data Protection compliance matters for their academies ○ Update Headteachers/Principal on trends, incidents and risks in relation to data protection within their academies ○ Be a point of contact for staff regarding Data Protection queries and issues within their academy ○ Participate in training and attend Data Network meetings
TRUST DIRECTOR OF IT	○ Manage backup and disaster recovery systems and report updates to the COO ○ Monitor for security incidents and cyber threats ○ Undertake regular security testing and vulnerability assessments

LGBs Accountable for monitoring and reviewing	○ Ensure their academy complies with Trust data protection policies ○ Monitor academy-level data protection risks ○ Review data breach incidents at academy level ○ Report Academy risks to Trust Board ○ Ensure local compliance with Trust policies and procedures ○ Challenges Headteacher/Principal on data protection implementation ○ Ensure adequate training for academy staff ○ Support data protection culture at academy level
Headteachers/Principals Responsible	○ Responsible for data protection compliance within their academy ○ Ensure all staff complete mandatory data protection training ○ Report data breaches to the CEO/COO/DPO as soon as they are aware ○ Manage SAR/FOI with DPO and Academy Data ○ Day-to-day management of Academy-level risk and mitigation ○ Report significant risks to LGB ○ Ensure secure handling of staff and learner personal data
Senior Leadership Teams Responsible	○ Support Headteacher/Principals in embedding data protection practices ○ Champion data protection throughout the academy and within their areas of responsibility ○ Report risks and mitigation to Headteacher/Principal ○ Monitor compliance with Trust and Academy policies and procedures
All Staff Responsible	○ Follow the Trust and Academy policies and procedures ○ Complete mandatory data protection training as directed ○ Report suspected data breaches immediately/within 24 hours ○ Only access personal data necessary for their role ○ Keep personal data secure [locked cabinets, strong passwords] ○ Follow secure protocols when sharing personal data outside of the academy/Trust ○ Maintain confidentiality of learner and staff information

Implementation

The Potteries Educational Trust will appoint a Data Protection Officer to act independently to ensure that there are no conflicts of interest. This may be through the appointment of an external provider.

The Potteries Educational Trust will ensure that:

- Regular monitoring reports are provided to the Trust Audit and Risk Committee.
- Briefings are held which introduce staff to the concept of Data Protection and to this policy; including staff induction, management team, and department team meetings; to enable ongoing dialogue around protecting personal data held by the Trust.

- Support staff with primary responsibility for processing of personal and sensitive information receive training appropriate to their day to day duties, and be required to maintain a level of operational understanding and awareness for the implementation of this policy and associated procedures. They will receive refresher training at the appropriate intervals.
- All Trust staff receive a level of training appropriate to their role, with refresher training at appropriated intervals. This will be recorded and monitored through central workforce development records.
- Information technologies are used to ensure that this policy is accessible to all users.

Communication

The policy is approved by the Board of Trustees.

The policy is communicated to all staff through staff induction, the staff intranet, virtual learning environment (VLE), email, mandatory training and refresher training on a 3-year cycle.

Awareness and acceptance of the policy is a requirement for new staff upon appointment. The policy is available on the staff intranet and on request to members of the public.

Users of the Trust's IT facilities and those with access to personal information receive a level of training appropriate to their role, with refresher training every 3 years.

All data subjects are kept informed of their rights regarding data protection through clear, simple information provided at the point of data collection, and through the Trust website.

Monitoring

The implementation and impact of the Data Protection Policy will be continuously monitored by each Headteacher/Principal with the support of the academy Data Protection Champion.

A Data Protection report will be presented by the COO each term to the Audit and Risk Committee providing a summary of all assurance and improvement actions taken in respect of data protection in the period since the last report, along with a summary of subject access requests received and responded to.

The Data Protection Policy is reviewed according to a documented programme of review by the Board of Trustees.

Associated Information and Guidance

Relevant legislation includes:

- Data Protection Act 2018 and General Data Protection Regulation (UKGDPR)
- Privacy and Electronic Communications Regulations (PECR)
- Data Use and Access Act 2025 (DUA Act)
- Data Protection (Processing of Sensitive Personal Data) Order 2000
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000

Further guidance

- The Information Commissioner's Office 'Guide to Data Protection Principles'

Related Documents

- Freedom of Information Policy
- IT Acceptable Use Policy
- Safeguarding Policy