DATA PROTECTION POLICY

Potteries Educational Trust

Policy Family	Information Governance
Reference	INF-01
Responsible Manager	Chief Information Officer
Approval Date	February 2024
Issue Number	4
Review Date	June 2025

Aim

The policy and associated procedures aim to ensure that personal data is collected, stored, transferred and disclosed only in compliance with applicable legislation, primarily the General Data Protection Regulation (The GDPR) Data Protection Act 2018 (The Act).

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, which includes a number of member and any associate member organisations. Collectively, the member organisations within the trust are referred to as The Trust.

Definitions

The Data Controller
The Potteries Educational Trust as a corporate body is the data controller, and the Corporation is ultimately responsible for the implementation of all appropriate policies and procedures to meet its obligations. Trustees, Local Governing Board Members, employed members of staff, agency workers, contractors and consultants are required to implement the Policy on behalf of the Trust, and are referred to throughout this document as 'Staff'.

The Data Processor
A person or other body, other than an employee of the Trust, who processes personal data on behalf of the data controller e.g. contractors or information system platforms. Where appointed the Controller remains responsible for what happens to the Personal Data.

Special categories of personal data

Personal data which is more sensitive and so needs more protection, including information about an individual's: Racial or ethnic origin; Political opinions; Religious or philosophical beliefs; Trade union membership

Data Protection Impact Assessments (DPIA)
A risk assessment in relation to the use of Personal Data for a new service, product or process. This must be done prior to the processing

Data Breach
A Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data.

Policy

Responsibilities

The Board of Trustees
The Potteries Educational Trust as a body corporate is considered to be the Data Controller under The Act, and the Board of Trustees are therefore ultimately responsible for approval, implementation and oversight of this policy within all member organizations.

The Chief Executive Officer

- To ensure the Trust Board has all necessary information and training to hold Executive Leaders to account in their Data Protection responsibilities.
- To support the CIO in reporting Data Protection risks and mitigations across the trust in line with the PET Data Protection Policy
- To ensure the Executive Team are supported to fulfil their statutory responsibilities as per the PET Data Protection Policy
- To ensure Data Protection Services provide effective value for money.

Headteachers and Principal(s) (prevention and compliance)

- To implement PET Policies and Procedures in their own academies.
- To ensure the Data Protection Champion has sufficient time and capacity to fulfil their responsibilities.
- To communicate and help staff with training to understand their responsibilities within the PET Data Protection Policy
- To be responsible for the management of personal data processed within their academies and ensure compliance with the PET Data Protection Policy and statutory requirements.
- To give appropriate time for the Data Protection Champions to attend trust training and network meetings to support them in their role
- To seek advice and guidance from the Chief Information Officer when required
- To ensure, when required, that the CIO has appropriate access to personal data and processing activities to share with the DPO Service where required

Data Protection Champions (operational management in own academy)

- Coordinate Data Protection compliance matters for their academies
- Keep Headteachers/Principal updated as to trends, incidents and risks regarding Data Protection issues within their academies
- Be a point of contact for staff regarding Data Protection queries and issues at their academy
- Update relevant Data Protection/IT security matters to the attention of staff in their academy

- Participate in training in Data Protection/IT security and attend Network meetings where appropriate. These will be booked well in advance to ensure that workload is not increased unnecessarily.
- Complete a Data Protection audit once a year and report findings to the Headteacher/Principal

Chief Information Officer (strategic oversight of compliance, prevention and management)

- To provide support and advice to Headteachers/Principal (SFC) on Data Protection issues
- Be the Trust point of contact with the Data Protection Officer/Service
- To escalate issues to the Data Protection Service on behalf of the Headteachers/Principal/CEO or other members of the Central Services Team.
- To report to Trustees once a term on behalf of the DPO Services
- Ensure the DPO operates independently as per statutory requirements

Data Protection Officer/Service (external and independent guidance and resolution of serious issues)

- Assist the Trust to monitor internal compliance
- Inform and advise on data protection obligations
- Provide advice regarding Data Protection Impact Assessments (DPIAs)
- Act as a contact point for data subjects and the Information Commissioner's Office (ICO).
- Manage serious information breeches, liaising with the ICO
- Keep the CIO and CEO informed and updated on the status and resolution of serious breaches or incidents.

All Staff

- Ensure that any personal data which they process is kept securely and personal information is not disclosed accidentally or otherwise to any unauthorized third party.
- Comply with the data protection principles defined under the Act and as set out in this policy.
- Be aware of and abide by this policy and associated guidance.
- Ensure that pupils using personal data for projects or coursework do so appropriately. This includes being compliant when storing data.

All Students and Staff

- Check that any information they provide the Trust about their studies/employment is accurate.
- Inform the Trust of any changes to the information they provided, e.g. change of address.
- Inform the Trust of any errors or changes in their personal information.

Data Protection Principles

When using Personal Data, Data Protection Laws require that the Trust complies with the following principles. These principles require Personal Data to be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
- accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;
- kept for no longer than is necessary for the purposes for which it is being processed; and

- processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In addition to complying with the above requirements, the Trust will demonstrate using relevant policies, guidance and documentation that it complies with them.

Data Protection by design and default

The Trust will adopt 'Data Protection by design and default' as best practice outlined in Data Protection legislation.

The Trust will ensure privacy issues are fully explored and addressed during project planning and process/system design stages and that appropriate technical and organisational measures are put in place to ensure that:

- processing activities are compliant with Data Protection legislation;
- the rights and interests of data subjects are protected.

This will be done by:

- All Trust stakeholders considering data protection in all their dealings by ensuring that the data the Trust takes or holds is kept secure (data by design)
- The Trust only collecting and holding data or information it needs for the purpose required (data by default)

Individuals' 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.

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.
- 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.
- 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.

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.

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.

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.

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 their Data Protection Champion, and receiving approval from their Headteacher/Principal.

The Trust does not carry out Automated Decision Making or Profiling in relation to its employees.

Implementation

The Data Protection Officer
The Trust will appoint a Data Protection Officer ensuring that there are no conflicts of interest between this role and their wider responsibilities within the Trust. Details of their name and contact details will be published on the Trust website as well as being widely available to all Staff and students. The DPO will operate independently of the leadership team and will not be penalised for performing their duties or reporting issues to the board. Adequate resources and frameworks will be provided to ensure that the DPO can perform their duties.

Data Protection Champions
The Trust will appoint a group of data protection champions, each of whom will support the headteacher/Principal to implement good practice and monitor compliance within a specific team or location. Data protection champions will be provided with specific training and support from the CIO to implement this policy and associated procedures for their areas of responsibility.

Training and Awareness
The Trust will

- Ensure all parties are aware of their responsibilities under the GDPR and are aware of associated College policies and procedures. Appropriate and regular training will be provided for all parties involved in using the College's data and systems.
- Data Protection training will be provided in the induction programme to present an overall picture of Data Protection regulations and the role of all staff in maintaining data confidentiality and the importance of data accuracy.
- Where appropriate local, departmental induction programmes will concentrate on specifics of their role and details on how Data Protection affects their job.
- Trainee teachers will be provided with details of their roles and responsibilities
- Training on aspects of data protection will be provided as part of normal systems training
- All parties will receive notification regarding changes to policies, standards and procedures on a timely basis.

Lawful Use of Personal Data

- The Trust will carefully assess how it uses all Personal Data and document this within the Information Asset Register.
- Any changes to the use of personal information will be approved by the Trustees in advance and documented through an update to the register.
- Where appropriate individuals will be notified of the change to the use of their personal data.

Special categories of personal data

- The privacy notices for all data subjects will provide clear information about sensitive personal data processed by the Trust, and the reasons for processing this data.
- Additional safeguards and security procedures will apply to the processing of this data.

Transparent Processing – Privacy Statements

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

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 Student 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.

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.

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.

Please 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).

Data Security

The Trust will:

- have security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data.
- have in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

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 students as part of their learning programme. This may include the recording of lessons and other activities, which may include images of teachers, students and other staff. Such images and recordings will be shared with staff and students 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 student 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 for example for the security or sharing of media, may differ from standard procedures. In particular, the Trust will;

- Ensure that all images of students 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;

Data Breaches

- Where there is a suspected data breach the Trust Data Breach procedure will be followed
- All suspected breaches will be investigated by the Data Protection Champion who will liaise with their Headteacher/Principal and, where appropriate reported to the CIO.
- All Data breaches (including near misses) will be recorded on the Trust Central Data breach register
- 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 CIO, who will report their findings to the appropriate Head teacher/Principal
- The Chair of the Audit Committee will be responsible for providing the Board of Trustees with a report of any breaches through the minutes of the Audit Committee and their presentation at Board meetings.

Data Protection Impact Assessments (DPIA)

- A DPIA will be completed according to the Trust's Data Protection Impact Assessment Procedure where the use of Personal Data is likely to result in a high risk to the rights and freedoms of Individuals.
- Where a DPIA reveals risks which are not appropriately mitigated the Information Commissioners Office (ICO) will be consulted.
- The Head teacher/Principal will be responsible for the review of all impact assessments for their academies, consulting as required with their Data Protection Champions.
- The Head teacher/Principal will be responsible for the approval of all changes to procedure once a DPIA has been completed and will consider the advice of their Data Protection

Champions and where necessary the CIO in making any decisions, including the steps required to mitigate any identified risks.

Transferring Personal Data to a Country Outside the United Kingdom

- Staff will not export Personal Data unless it has been approved by their Data Protection Champion, who will advise if any proposed storage or transfer is likely to result in a transfer out of the UK.
- All transfers of data outside of the UK will be subject to a DPIA with particular focus on the risks to data security and any alternative processing methods available to eliminate these risks.

Records Management

- At the end of the agreed period for each type of information recorded, also referred to as an Information Asset, the Trust will take steps to delete such information from its information systems, databases and electronic files, and to destroy paper records using agreed, secure processes.
- The agreed retention period for each type of information, and the reasons for this will be documented in the Information Asset Register, which provides a central record of all information processed by the Trust.

When setting retention periods, consideration will be given to the following key factors:

- The purpose for which the data was obtained;
- Any specific consents provided by the data subject in relation to the use or retention of that data;
- Whether the original purpose has been fulfilled; and
- Whether the data needs to be retained to support any potential legal process

Third Party Relationships

If the Trust appoints a contractor who is a Processor of the Trust's Personal Data sufficient due diligence will be carried out.

Any contract where an organisation appoints a processor will be in writing and the following obligations will be put in place:

- to only act on the written instructions of the Trust;
- to not export Personal Data without the Trust's instruction;
- to ensure Staff are subject to confidentiality obligations;
- to take appropriate security measures;
- to only engage sub-processors with the prior consent (specific or general) of the Trust and under a written contract;
- to keep the Personal Data secure and assist the Trust to do so;
- to assist with the notification of Data Breaches and Data Protection Impact Assessments;
- to assist with Subject Access/Individuals rights;
- to delete/return all Personal Data as requested at the end of the contract;
- to submit to audits and provide information about the processing;
- to tell the Trust if any instruction is in breach of the GDPR or other European Union or member state data protection law.

In addition, contracts between The Trust and any data processor should set out: the subject-matter and duration of the processing; the nature and purpose of the processing; the type of Personal Data and categories of Individuals; and the obligations and rights of the Controller.

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. This is recorded and monitored through central Workforce Development records.

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 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 CIO each half term to the Audit 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)
- Human Rights Act 1998
- Data Protection (Processing of Sensitive Personal Data) Order 2000
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)

Further guidance:

- The Information Commissioner's Office "Guide to Data Protection" (https://ico.org.uk/for-organisations/guide-to-data-protection/)
- The JISC "Data protection" guide (https://www.jisc.ac.uk/guides/data-protection)

Related Documents

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