DATA PROTECTION POLICY

Potteries Educational Trust

Policy Family	Information Governance
Reference	INF-01
Responsible Manager	Data Protection Officer
Approval Date	June 2021
Issue Number	2
Review Date	June 2023

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).

Scope

The policy and associated operating procedures apply to The Potteries Educational Trust, which includes a number of member and associate member organisations. Collectively, the member organisations within the trust are referred to as The Trust.

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 organisations. Their responsibilities are for ensuring that data is collected, stored and processed fairly, for deciding which types of information will be processed and the reasons for processing.

The Data Protection Officer

The Data Protection Officer has overall responsibility for the implementation of this policy, and is responsible for providing advice, developing data protection guidance and raising awareness of data protection matters across the Trust. The data protection officer will be responsible for informing and advising the Board of Trustees and staff of their obligations to comply with the GDPR, the Act and other data protection laws. The DPO will monitor compliance with the GDPR and other laws, advise on data protection impact assessments and ensure that training is provided to all members of staff.

The Chief Executive Officer and Senior Leadership Teams

It is the responsibility of the Chief Executive Officer and Senior Leadership Teams in each Academy to recommend this policy for approval, approve any associated procedures, ensure compliance with the policy and procedures, and to provide training and communication to ensure that all staff understand the policy. Additionally they are responsible for the management of personal data processed within their areas of responsibility and for encouraging good information governance practice across the Trust.

All Staff

All staff are responsible for ensuring that any personal data which they process is kept securely and personal information is not disclosed accidentally or otherwise to any unauthorised third party.
If and when, as part of their responsibilities, staff collect information about other people, they must comply with the data protection principles, defined under the Act and as set out in this policy.
All staff have a responsibility to make themselves aware of and abide by this policy and associated guidance.

All Students and Staff

Students and staff are responsible for ensuring that all personal data provided to the Trust is accurate and kept up to date. It is their responsibility for informing the Trust when this changes.

This includes but is not limited to:

- Checking that any information that they provide to the Trust in connection with their employment is accurate.
- Informing the Trust of any changes to information, which they have provided, e.g. change of address.
- Informing the Trust of any errors or changes in their personal information.

1. Data Protection Law

This policy is informed by and meets the requirements of The UK General Data Protection Regulation and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

2. 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'.

3. 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 report to the Board of Trustees. 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 will be provided to ensure that the DPO can perform their duties, including support from a wider group of Data Protection Champions within teams that undertake significant data processing activities.

4. Data Protection Champions

The Trust will appoint a group of data protection champions, each of whom will support the Data Protection Officer 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 DPO to implement this policy and associated procedures for their areas of responsibility.

5. 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:

1) processed lawfully, fairly and in a transparent manner;
2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3) adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
4) 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;
5) kept for no longer than is necessary for the purposes for which it is being processed; and
6) 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 also has to demonstrate in writing that it complies with them. The Trust has a number of policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that the Trust can demonstrate its compliance.

6. Lawful Use of Personal Data

In order to collect and/or use Personal Data lawfully, the Trust needs to be able to show that its use meets one of a number of legal grounds. In addition, when the Trust collects and/or uses Special Categories of Personal Data, it has to show that one of a number of additional conditions is met.
The Trust will carefully assess how it uses all Personal Data and document this within the Information Asset Register. If the Trust changes how it uses Personal Data, it needs to update this record and may also need to notify Individuals about the change. Any changes to the use of personal information must therefore be approved by the Data Protection Officer in advance, and documented through an update to the register.

7. Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, ethnicity, gender other sensitive, or special category data. The privacy notices for all data subjects will

provide clear information about the 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.

8. 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 College website.

If the Trust changes how it uses Personal Data, the Trust may need to notify Individuals about the change. If Staff, therefore, intend to change how they use Personal Data they must notify the Data Protection Officer who will decide whether the intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

9. Exchange of Personal Information with 3rd Parties

The Trust is a publically funded organisation and must disclose certain information to funding bodies and other government approved organisations. 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. Under no circumstances will the Trust disclose or sell personal information to third parties for the purposes of marketing, sales of goods and services or promotions.

10. Data Quality

Data Protection Laws require that the Trust only collects and processes Personal Data to the extent that it is required for the specific purpose(s) notified to the Individual in a privacy statement and as set out in the Trust's Information Asset Register. The Trust is also required to ensure that the Personal Data the College holds is accurate and kept up to date.

All Staff that collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.

All Staff that obtain Personal Data from sources outside the Trust shall take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date and is limited to that which is adequate, relevant and limited to what is 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.
In order to maintain the quality of Personal Data, all Staff that access Personal Data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. 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).

The Trust recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws.

11. Data Security

The Trust takes information security very seriously and the Trust has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The Trust has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

12. Use of CCTV

The Trust's use of CCTV is regulated by a separate Code of Practice. For reasons of personal security and to protect Trust premises and the property of staff and students, closed circuit television cameras are in operation throughout our buildings. The presence of these cameras may not be obvious. This policy determines that personal data obtained during monitoring will be processed as follows:

- recordings are only kept as long as required to ensure adequate history is available to investigate concerns
- any live or pre-recorded monitoring will be carried out only by a limited number of specified staff;
- personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete;
- Staff involved in monitoring will maintain confidentiality in respect of personal data.

13. 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.

14. Right of Access - Subject Access Requests

Individuals have the right under Data Protection Law to ask the Trust to confirm what Personal Data they hold in relation to them and provide them with a copy of the data. All Subject Access Requests will be directed by Trust Staff to the Data Protection Officer 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.

To comply with The GDPR and UK Law, the Trust will aim to respond to all subject access requests within 30 days of receipt. In the event that a request cannot be fully answered within that period, the trust will;

- Seek to clarify the nature and scope of the request in order 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.

15. Right of Erasure (Right to be Forgotten)

This is a limited right for Individuals to request the erasure of Personal Data concerning them where the use of the Personal Data is no longer necessary; their consent is withdrawn and there is no other legal ground for the processing; the individual objects to the processing and there are no overriding legitimate grounds for the processing; the Personal Data has been unlawfully processed; or the Personal Data has to be erased for compliance with a legal obligation.

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 individual has a right 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.

16. Right of Data Portability

An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine-readable format, where the processing is based on consent or on a contract; and the processing is carried out by automated means. This right isn't the same as subject access and is intended to give Individuals a subset of their data.

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.

17. Right of Rectification and Restriction

Finally, Individuals are also given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances. 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. The Data Protection Officer will investigate any cases where an individual feels that their rights, including to the rectification of incorrect information or the restriction of use, have not been met.

18. Marketing and Consent

The Trust will sometimes contact Individuals to send them marketing or to promote the Trust. 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 particular 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.

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.

19. 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 the Data Protection Officer.
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 a member of the Senior Management Team.

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

20. Data Protection Impact Assessments (DPIA)

The GDPR introduces a new requirement to carry out 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 via a Data Protection Impact Assessment (DPIA).

A DPIA must 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) must be consulted. The Data Protection Officer will be responsible for the review of all impact assessments and consultation as required with the ICO.

The Senior Management Team will be responsible for the approval of all changes to procedure once a DPIA has been completed, and will take into account the advice of the DPO in making any decisions, including the steps required to mitigate any identified risks.

21. Transferring Personal Data to a Country Outside The European Economic Area (EEA)

Data Protection Laws impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EEA but also includes storage of Personal Data or access to it outside the EEA. So that the Trust can ensure it is compliant with Data Protection Laws, Staff must not export Personal Data unless it has been approved by the Data Protection Officer, who will advise if any proposed storage or transfer is likely to result in a transfer out of the EEA. All transfers of data outside of the EEA will be subject to a DPIA with particular focus on the risks to data security and any alternative processing methods available in order to eliminate these risks.

22. Records Management

The Trust has a legal responsibility not to keep personal data for longer than needed for the specific purposes agreed when it was collected. At the end of the agreed period for each type of information, 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 are 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**

23. Appointing Contractors Who Access the Trust's Personal Data

If the Trust appoints a contractor who is a Processor of the Trust's Personal Data, Data Protection Laws require that the Trust only appoints them where the Trust has carried out sufficient due diligence and only where the Trust has appropriate contracts in place.

Any contract where an organisation appoints a Processor must be in writing.

The Trust is considered as having appointed a Processor where you engage someone to perform a service for you and as part of it they may get access to your Personal Data. Where you appoint a Processor you, as Controller remain responsible for what happens to the Personal Data.

Data Protection Law requires all contracts with a Processor to contain the following obligations as a minimum: to only act on the written instructions of the Controller; to not export Personal Data without the Controller'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 Controller and under a written contract; to keep the Personal Data secure and assist the Controller 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; and to tell the Controller 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.

24. Data Breach

Whilst the Trust takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. This is referred to as a Personal Data breach and Staff must comply with the Trust's Data Breach Notification Procedure. All Staff are required to understand the

internal reporting process for personal data breaches, and comply with the strict timeframes set out within the procedure.

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. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of actions taken by someone within the organisation.

Any breach of data protection procedures, which must be reported to the ICO immediately upon discovery, will be reported in parallel to the Principal and Chief Executive, the Chair of the Corporation Board, and the Chair of the Audit Committee by the Data Protection Officer.
All breaches will be investigated formally by the Data Protection Officer and reported to the Audit Committee. 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 Officer, the investigation will be undertaken by the Clerk to the Corporation, who will report their findings to the Audit Committee as above.
The Chair of the Audit Committee will be responsible for providing the Board of Trustees with a report of any breaches or issues in relation to Data Protection through the minutes of the Audit Committee and their presentation at Board meetings.

Implementation

The Potteries Educational Trust will ensure that:

1) The Data Protection Officer has a direct line of reporting to the Audit Committee of the Board of Trustees.
2) Briefings are held which introduce Staff to the concept of a Data Protection Policy 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.
3) 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 every 2 years.
4) All Trust staff receive a level of training appropriate to their role, with refresher training every 3 years. This will be recorded and monitored through central Workforce Development records.
5) 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. This is recorded and monitored through central Workforce Development records.

All data subjects are kept informed of their rights with regard to data protection through clear, simple information provided at the point of data collection, and through our public facing web page http://stokesfc.ac.uk/dataprotection.

Monitoring

The Trust has appointed a designated Data Protection Officer with specific responsibilities and accountability for data protection across the Trust.

The Data Protection Officer will be supported in managing the framework for data protection by named Data Protection Champions with existing responsibility for ICT Services, Student Records, Marketing and Human Resources. In discharging these duties, Data Protection Officer will have a direct line of reporting through the Clerk to the Board of Trustees to the Audit Committee of the Board.

A Data Protection report will be presented to every meeting of 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 implementation of the Data Protection Policy is continuously monitored by the Data Protection Officer and managers including the IT Services Manager who has responsibility for Information Security.

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

Associated Information and Guidance

Relevant legislation includes:

- Data Protection Act 2018
- 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