



# Data Protection and Data Subject Rights Policy

Date	Revision & Amendment Details	By Whom
December 2022	Approved	Business and Finance Committee
January 2024	Reviewed and approved	Business and Finance Committee

## CONTENTS

<b>Part 1 – Data Protection Policy</b>	<b>3</b>
1 Introduction	3
2 Scope	3
3 Definitions	4
4 Data Protection Principles	4
5 Lawfulness, Fairness and Transparency	5
6 Purpose Limitation	6
7 Data Minimisation	7
8 Accuracy	7
9 Storage Limitation	7
10 Integrity and Confidentiality	8
11 Documentation and Records	8
12 Individual Obligations	9
13 International Transfer	9
14 Training	9
15 Working remotely	9
16 Consequences of Failing to Comply	10
17 Contact	10
<b>Part 2: Data Subject Rights Policy</b>	<b>10</b>
18 Data Subject Rights and Requests	10
19 Subject Access Requests	11
20 Right to Rectification	12
21 Right to Erasure	13
22 Right to Restrict Processing	13
23 Right to Object	14
24 Right to Data Portability	15
25 Monitoring Arrangements	15

## PART 1 – Data Protection Policy

### 1. Introduction

Peterborough Diocese Education Trust (“**the Trust**”) is committed to complying with its data protection obligations, and to being concise, clear and transparent about how it obtains and uses personal information relating to the Trust community, including pupils, parents and staff.

This policy sets out how we comply with our data protection obligations set out in the UK General Data Protection Regulation (the “**UK GDPR**”) and the Data Protection Act (“**DPA**”) 2018, and seek to protect the personal data of our pupils, parents, staff, and other individuals who may come into contact with the Trust.

The aim of this policy is to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal data to which they may have access in the course of their duties.

The Trust has appointed Angela Corbyn as the person with overall responsibility for data protection compliance (the Data Protection Officer (“**DPO**”). Any questions about this policy or requests for further information should be directed to them. The DPO may be contacted using the following details:

- Angela Corbyn: [dpo@pdet.org.uk](mailto:dpo@pdet.org.uk) or [Tel:07775436141](tel:07775436141)

### 2. Scope

This policy applies to all staff. **Any reference to the term staff in this policy includes employees, governors, directors, volunteers, consultants, contractors, any peripatetic workers and sports coaches, and supply teachers.**

Staff should refer to the Trust’s privacy notices and, where appropriate, to other relevant policies including those relating to information security, data retention, acceptable use , and personal data breaches, which contain further information regarding the protection of personal data in those contexts.

This policy does not form part of any employee’s contract of employment or consultant’s consultancy agreement and we may amend, update or supplement it from time to time. We will circulate any new or materially modified policy to staff when it is adopted.

All staff are required to read and confirm that they understand this policy.

### 3. Definitions

This policy uses the following definitions:

Term	Meaning
<b>Criminal offence data</b>	Means all personal data relating to criminal convictions and offences or related security measures (including information about criminal activity, allegations or suspicions, investigations and proceedings).
<b>Data subject</b>	Means an individual to whom personal data relates.
<b>Personal data</b>	Means any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other available information.
<b>Personal data breach</b>	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal or special category data transmitted, stored or otherwise processed.
<b>Processed / Processing</b>	Means any actions performed on personal data, including collecting, recording, organising, structuring, storing, modifying, consulting, using, publishing, combining, erasing, and destroying data.
<b>Special category personal data</b>	Means personal data afforded special protection by the UK GDPR. This includes, information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an individual), information concerning an individual's health and sex life or sexual orientation.
<b>Information Commissioner's Office (ICO)</b>	Means the UK's data protection and information regulator.

### 4. Data Protection Principles

When processing personal data, the Trust and its staff must comply with the data protection principles set out in Article 5 of the UK GDPR as follows:

- We will process personal information lawfully, fairly and in a transparent manner (**'lawfulness, fairness and transparency'**)
- We will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes (**'purpose limitation'**)
- We will only process the personal information that is adequate, relevant and necessary for the relevant purposes (**'data minimisation'**)

- We will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal data is deleted or corrected without delay (*'accuracy'*)
- We will keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed (*'storage limitation'*); and
- We will take appropriate technical and organisational measures to ensure that personal data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage (*'integrity and confidentiality'*).

In addition, the Trust is also responsible for, and must be able to demonstrate compliance with the above principles (*'accountability'*). This means that the Trust will:

- Inform individuals about how and why we process their personal data, usually by way of a privacy notice
- Be responsible for checking the quality and accuracy of the information
- Regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with our records retention policy
- Ensure that when information is authorised for disposal it is disposed of / deleted appropriately
- Ensure appropriate security measures to safeguard personal information whether it is held in paper files or electronically, and follow the requirements set out in our information security policy at all times
- Share personal information with others only when it is necessary and legally appropriate to do so
- Set out clear procedures for responding to requests for access to personal information known as subject access requests and other rights exercised by individuals in accordance with the UK GDPR (please see "Part 2: Data Subject Rights Policy" below); and
- Report any actual or suspected personal data breaches in accordance with the procedure set out in the Trust's Procedure for Reporting Personal Data Breaches.

## 5. Lawfulness, Fairness and Transparency

The Trust is responsible for ensuring that personal data is processed in a lawful, fair and transparent way. In relation to any processing activity we will, before the processing begins, and then regularly while it continues:

- Review the purposes of the particular processing activity, and identify which of the following legal bases for processing (as set out in Article 6 of the UK GDPR) is most appropriate:
  - that the data subject has *consented* to the processing
  - that the processing is necessary for the *performance of a contract* to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
  - that the processing is necessary for *compliance with a legal obligation* to which the Trust is subject
  - that the processing is necessary for the *protection of the vital interests* of the data subject or another natural person

- that the processing is necessary for the purposes of *legitimate interests* of the Trust or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.
- Except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose)
- Include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s)
- Where special category personal data or criminal offence data is processed, also identify a lawful condition (as set out in Articles 9 and 10 of the UK GDPR, and Schedule 1 of the DPA 2018) for processing this type of information, and document it.

When determining whether the legal basis of legitimate interests is appropriate, we will:

- Carry out a legitimate interests assessment (“LIA”) (a type of light-touch risk assessment) and keep a record of it, to ensure that we can justify our decision
- If the LIA identifies a significant risk to an individual’s data protection rights, consider whether we also need to conduct a data protection impact assessment (“DPIA”)
- Keep the LIA under review, and repeat it if circumstances change; and
- Include information about our legitimate interests in our relevant privacy notice(s).

Where processing of personal data is likely to result in a high risk to individuals, we will, before commencing the processing, carry out a DPIA to assess:

- Whether the processing is necessary and proportionate in relation to its purpose
- The risks to individuals; and
- What measures can be put in place to address those risks and protect personal information.

In order to comply with our transparency obligations, the Trust will issue privacy notices from time to time, informing data subjects about the personal data that we collect and hold, how they can expect personal data to be used and for what purposes. We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

## 6. Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with the purpose(s) identified.

Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and, where necessary, they have consented.

## 7. Data Minimisation

The Trust will ensure that the processing of personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Personal data should only be collected to the extent required for the relevant duties, and it should be ensured that any personal data collected is adequate and relevant for the intended purposes. In order to do this:

- The processing of personal data should be minimised, for example, through redaction (i.e. obscuring or censoring text) and the deletion of long emails trails
- Personal data should be anonymised where appropriate
- Personal data should be pseudonymised where possible, for example, through the use of initials rather than full names; and
- Ensure that when personal data is no longer needed, it is deleted in accordance with the Records Retention Policy.

## 8. Accuracy

Personal data must be accurate and kept up to date. It must be corrected or deleted without delay when it is inaccurate.

Staff have a responsibility for helping the Trust keep their own personal data up to date. Staff should let HR know if the information they have provided to the Trust changes, for example if they move house or change details of the bank or building society account to which they are paid. This helps the Trust comply with its wider data protection obligations and can reduce the likelihood of a data breach occurring. The Trust also asks parents / carers to inform them of any changes to their or their child's personal data.

## 9. Storage Limitation

Personal data should not be kept for any longer than is necessary for the purposes for which the personal data is processed.

The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow guidance contained in the Records Retention Policy, which sets out the relevant retention period, or the criteria that should be used to determine the retention period.

Personal information that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

## 10. Integrity and Confidentiality

The Trust will use appropriate technical and organisational measures in accordance with our information security policy to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of the DPO to the use of data in the way envisaged.

All staff have an obligation to report actual or suspected personal data breaches to the DPO immediately upon discovery. Please refer to the Trust's Procedure for Reporting Personal Data Breaches for further guidance on reporting procedures and obligations.

## 11. Documentation and Records

We will keep written records of processing activities which are high risk, i.e. which may result in a risk to individuals' rights and freedoms or involve special category data or criminal offence data, including:

- The purposes of the processing
- A description of the categories of individuals and categories of personal data
- Categories of recipients of personal data
- Where relevant, details of transfers of personal data outside the UK, including documentation of the transfer mechanism safeguards in place
- Where possible, retention schedules; and
- Where possible, a description of technical and organisational security measures.

As part of our record of processing activities we document, or link to documentation, on:

- Information required for privacy notices
- Records of consent
- Controller-processor contracts
- The location of personal information
- DPIAs
- Records of personal data breaches; and
- Records of individual rights.

If we process special category data or criminal offence data, we will keep written records of:

- The relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose
- The lawful basis and additional conditions relied upon to process this information; and

- Whether we retain and erase the personal information in accordance with our Records Retention Policy and, if not, the reasons for not following the Records Retention Policy.

We will conduct regular reviews of the personal information we process and update our documentation accordingly.

## **12. Individual Obligations**

Staff may have access to the personal information of other members of staff, as well as pupils, parents, volunteers and visitors in the course of their employment or engagement. If so, the Trust expects staff to help meet its data protection obligations to those individuals.

If staff have access to personal data, they must:

- Only access the personal data that they have authority to access, and only for authorised purposes
- Only allow other staff to access personal data if they have appropriate authorisation
- Only allow individuals who are not staff to access personal data if you have specific authority to do so from the DPO
- Keep personal data secure (e.g. by complying with the obligations set out in the Acceptable Use Policy and IT Controls (Information Security) Policy; and
- To the extent that they may use personal devices for work purposes, comply with the Trust's Acceptable Use Policy.

## **13. International Transfers**

The Trust may transfer personal data outside the UK on the basis that that country, territory or organisation is designated as having an adequate level of protection, or that the organisation receiving the information has provided adequate safeguards to ensure the protection of personal data.

## **14. Training**

The Trust will ensure that staff are adequately trained (at least bi-annually) regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

## **15. Working Remotely**

As part of our commitment to flexible working, the Trust supports homeworking in appropriate circumstances, either occasionally (to respond to specific circumstances or to complete particular tasks) and in some cases on a regular basis (full or part-time).

Working remotely can lead to increased risk in terms of the security of Trust information (including personal data) and communications systems. When working remotely, staff must comply with all relevant policies, including our:

- Staff Data Protection Policy (this policy)
- IT Controls (Information Security) Policy
- Records Retention Policy
- Staff Code of Conduct
- Acceptable Use Policy (AUP) ; and
- Remote Education: Online Safety  
at all times and must attend any additional training on data protection and confidentiality as may be required by the Trust.

## 16. Consequences of Failing to Comply

The Trust takes compliance with this policy very seriously. Failure to comply with the policy:

- Puts at risk the individuals whose personal information is being processed
- Carries the risk of significant sanctions for the individual and the Trust; and
- May, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy any failure to comply with any requirement of it may lead to disciplinary action, which may result in termination of the member of staff's relationship with the Trust.

## 17. Contact

If anyone has any concerns or questions in relation to this policy, they should contact the DPO using the contact details above.

## Part 2: Data Subject Rights Policy

### 18. Data Subject Rights and Requests

Data subjects have rights in relation to their personal data. This includes the right to:

- Be **informed** about how, why and on what basis that information is processed (the Trust usually provides this information to data subjects via its Privacy Notice(s))
- Obtain confirmation that information is being processed and to obtain **access** to it and certain other information by making a subject access request
- Have personal data **corrected** if it is inaccurate or incomplete (known as *the right of rectification*)
- Have personal data **erased** in certain circumstances (sometimes known as *the right to be forgotten*)
- **Restrict the processing** of their personal data in certain circumstances (e.g. if there is a complaint about accuracy)

- **Object** to the processing of their personal data in certain circumstances
- **Receive** personal data that they have provided in a structured, commonly used and machine-readable format and to request that their personal data is **transferred** to another organisation (known as *the right to data portability*).

## 19. Subject Access Requests

Anybody has the right to ask the Trust for a copy of any personal information held about them, together with other information about how their information is used (known as supplementary information (see section below)). This legal right is called the right of access, often referred to as a subject access request or SAR.

- There are some legal exemptions that mean that requesters may not always be entitled to a copy of all of their personal information that we hold.

As part of a subject access request, data subjects are entitled to the following supplementary information:

- Whether their personal data is being processed by the Trust
- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom their personal data have been or will be disclosed
- The envisaged period for which the data will be stored or where that is not possible, the criteria used to determine how long the data are stored
- The existence of a right to request rectification or erasure of personal data or restriction of processing or to object to the processing
- Their right to lodge a complaint with the ICO
- Where the personal data are not collected from the individual, any available information as to their source; and
- Details of the safeguards in place for any transfers of their data to locations outside the UK.

If a member of staff receives a SAR from a pupil, parent or carer or other person, they should immediately forward it to the DPO who will support them through the process. The Trust has a legal duty to deal with SARs without delay and at the latest within one month of receipt (subject to the rights of the Trust to extend the time limit for response by a further two months, considering the complexity and number of the requests, in accordance with Article 12(3) of the UK GDPR).

Any individual, including a child or young person, may appoint another person to request access to their records. In such circumstances the Trust must have written evidence that the individual has authorised the person to make the request and the DPO must be confident of the identity of the individual making the request.

Where a child or young person lacks capacity to understand their rights and the implications of making a subject access request (e.g. due to their age or some other reason) a third party, such as a parent or carer, can make a request on their behalf. The DPO must, however, be satisfied that:

- The child or young person lacks sufficient understanding of their own data rights; **and**
- The request made on behalf of the child or young person is made in the child or young person's best interests.

Access to personal data may be restricted or refused in instances where an exemption under the DPA 2018 applies. For example, the relevant information is covered by legal advice privilege or information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s). The Trust must decide whether to apply any potential exemption (taking legal advice where appropriate), based on the circumstances of a particular request.

A subject access request may be made verbally, in writing or via the school / Trust's social media channels. Where possible, the Trust prefers requests to be made in writing. The Trust may ask the data subject for any further information reasonably required to locate the information.

All files must be reviewed and applicable exemptions under the UK GDPR and the DPA must be applied by the DPO. Any disclosure can only take place after the response is approved by the DPO. Any response sent to the requestor must comply with the requirements of the UK GDPR and must include the supplementary information the requestor is entitled to

Where some of the data in a document cannot be disclosed a copy of the full document and the altered document should be retained, with the reason why the document was altered.

## **20. Right to Rectification**

Data subjects have the right to request the rectification of inaccurate or incomplete data verbally or in writing. Any request for rectification should be sent to the DPO immediately.

Where personal data is identified as inaccurate or incomplete, it will be amended and the data subject notified of the same without undue delay and in any event within one month (unless this deadline is extended in accordance with the UK GDPR).

Where a request is refused, the request and reasons for refusal will be documented and notice of refusal should be provided to the individual within a month of receipt of the request. The Trust will include in its response the reasons why the request has been refused and information about the individual's right to complain to the ICO and to bring a civil claim.

## 21. Right to Erasure

Individuals have a right, in certain circumstances, to have their personal data permanently erased. Individuals may exercise this right in writing or verbally.

The right to erasure is also known as the 'right to be forgotten' and arises in the following circumstances:

- Where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed
- Where consent is the legal basis for processing and that consent is withdrawn
- Where legitimate interests is the legal basis for processing and the individual objects to the processing of their data, and there is no overriding legitimate interest to continue processing
- Where the Trust is processing the personal data for direct marketing purposes and the individual objects to that processing
- Where personal data is being unlawfully processed
- Where there is a legal obligation on the Trust to delete the personal data; or
- Where the Trust has processed the personal data to offer information society services to a child.

Any request for erasure should be sent to the DPO immediately. The request must be complied with within one calendar month (unless this deadline is extended in accordance with the UK GDPR).

The DPO will determine the outcome of any request for erasure of personal data. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, the Trust will inform those organisations of the request unless this proves impossible or involves disproportionate effort.

Where a request is refused, the Trust will inform the individual without undue delay and within one month of receipt of the request. The response will include the reasons for the refusal and information about the individual's right to complain to the ICO and to bring a civil claim.

## 22. Right to Restrict Processing

In the following circumstances, individuals have the right to request the restriction or suppression of their personal data in writing or verbally:

- Where the accuracy of personal data has been contested, during the period when the Trust is attempting to verify the accuracy of the data
- Where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure
- Where personal data would normally be deleted, but the individual has requested that their personal data be kept for the purpose of the establishment, exercise or defence of a legal claim
- Where there has been an objection to the processing, pending the outcome of any decision.

Any request for restriction should be sent to the DPO immediately. The request must be complied with within one calendar month (unless this deadline is extended in accordance with the UK GDPR).

The DPO will determine the outcome of any request for restriction of processing personal data. As matter of good practice, the Trust will automatically restrict the processing whilst considering the accuracy or legitimate grounds for processing the personal data in question.

Where processing has been restricted, such personal data will (with the exception of storage) be processed only in the following circumstances:

- With the consent of the data subject
- Where processing is necessary for the establishment, exercise or defence of legal claims
- For the protection of rights of another person (including a company); or
- For reasons of important public interest.

If the Trust has disclosed the personal data in question to others, it will contact each recipient to inform them of the restriction, unless this proves impossible or involves disproportionate effort.

Once the Trust has determined the accuracy of the data, or whether the Trust's legitimate grounds override those of the data subject, the Trust may decide to lift the restriction. The Trust will inform the requestor before the restriction is lifted.

Where a request is refused, the Trust will inform the individual without undue delay and within one month of receipt of the request. The response will include the reasons for the refusal and information about the individual's right to complain to the ICO and to bring a civil claim.

### **23. Right to Object**

Where personal data is being processed for direct marketing purposes, an individual has the right to object at any time to processing of their personal data for such purposes. This right is absolute and where such an objection is made the Trust will stop processing personal data for this purpose.

An individual also has the right to object to the processing of their personal data on the legal basis of:

- A task carried out in the public interest
- The exercise of official authority vested in the Trust; or
- The legitimate interests of the Trust or a third party.

Where such an objection is made, it must be sent to the DPO immediately. The DPO will assess whether the processing should cease or whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals concerned, or whether the information is required for the establishment, exercise or defence of legal proceedings.

The DPO is responsible for notifying the individual of the outcome of their assessment without undue delay and within one calendar month of receipt of the objection (unless this deadline is extended in accordance with the UK GDPR). If the request is refused, the response will include the reasons for the refusal and information about the individual's right to complain to the ICO and to bring a civil claim.

## **24. Right to Data Portability**

Individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format, and to require the Trust to transmit that personal data directly to another data controller in certain circumstances (where feasible).

If such a request for this is made, it should be forwarded to the DPO immediately and this will be reviewed and actioned as necessary.

## **25. Monitoring Arrangements**

This policy will be reviewed every three years but may be reviewed / updated as and when necessary / appropriate prior to then (e.g. a change in the law or statutory guidance).