



GDPR Policy and Procedures (Data Protection)

This policy was agreed by the Management Committee: Spring 2025

This policy will be reviewed: Spring 2026

Contents

1. Aims	3
2. Legislation and Guidance	3
3. Definitions	3
4. The Data Controller	4
5. Data Protection Principles	4
6. Roles and responsibilities.....	5
7. Privacy/Fair Processing Notice	5
8. Subject Access Requests.....	7
9. Parental Requests to see the Educational Record.....	7
10.Data Accuracy.....	7
11.CCTV.....	7
12. Biometric recognition.....	8
13. Artificial Intelligence.....	8
14. Storage of records.....	8
15. Disposal of Records	9
16. Data Breaches.....	9
17. Training	9
18. Monitoring Arrangements	10
19. Links with other policies	10
20.Contac information	10
21. Policy update information	11

Appendix

1. Photography and videos
2. Breach procedure

1. Aims

The PRU aims to ensure that all data collected about staff, students, parents and visitors is collected, stored and processed in accordance with the General Data Protection Regulation (UK GDPR).

This policy applies to all data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

This policy meets the requirements of Data Protection Legislation, and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education;

UK General Data Protection Regulation (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).

This policy is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

This policy also covers requirements of Keeping Children Safe in Education (paragraphs 141 and 142 Filtering and Monitoring).

It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: <ul style="list-style-type: none">• Contact details• Racial or ethnic origin• Political opinions• Religious beliefs, or beliefs of a similar nature• Where a person is a member of a trade union• Physical and mental health• Sexual orientation

	<ul style="list-style-type: none"> • Whether a person has committed, or is alleged to have committed, an offence • Criminal convictions
Processing	Obtaining, recording, storing, altering or destruction data
Data subject	The living individual whose personal data is held or processed
Data controller	A person or organisation that determines the purpose for which, and the way personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

4. The Data Controller

The PRU processes personal information relating to students, staff, parents, students' emergency contacts and visitors, and, therefore, is a data controller.

The PRU is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

5. Data Protection Principles

The UK GDPR is based on the following data protection principles, or rules for good data handling:

- Data shall be processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.
- 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.

6. Roles and responsibilities

The Management Committee has overall responsibility for ensuring that the PRU complies with its obligations under the UK GDPR.

Day-to-day responsibilities rest with the Executive Headteacher and The Operations Manager. The Operations Manager will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the PRU of any changes to their personal data, such as a change of address.

Data breach reporting is mandatory under the UK GDPR and all staff are aware of their obligation to report data breaches without delay.

7. Privacy/Fair Processing Notice

7.1 Students and parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the PRU is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, Local Authorities, the Department for Education and the National Health Service.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on student characteristics, such as ethnic group or Special Educational Needs and Disabilities
- Exclusion information
- Details of any medical conditions

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this Policy.

We are required, by law, to pass certain information about pupils to specified external bodies, such as our Local Authority and the Department for Education, so that they can meet their statutory obligations.

7.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, the PRU. The purpose of processing this data is to assist in the running of the PRU, including to:

- enable individuals to be paid
- facilitate safer recruitment practice
- support the effective performance management of staff
- improve the management of workforce data across the education sector
- inform our recruitment and retention policies
- allow better financial modelling and planning
- enable monitoring of people with, and without, Protected Characteristics under the Equality Act
- support the work of the School Teachers' Review Body

Staff personal data includes, but is not limited to, information such as:

- contact details, next of kin
- National Insurance numbers
- salary information
- qualifications
- absence data
- personal characteristics/protected characteristics
- medical information
- outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to. This may include advisers such as our Occupational Health and our Human Resources advisers.

We are required, by law, to pass certain information about staff to specified external bodies, such as our Local Authority and the Department for Education, so that they can meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the PRU holds should contact the Operations Manager in the first instance.

8. Subject Access Requests

Under the UK GDPR, Staff, Students and Parents\Carers have a right to request access to information the school holds about them. This is known as a Subject Access Request (SAR).

Subject Access Requests must be submitted in writing, either by letter or email. Requests should include:

- The subjects name
- A correspondence address
- A contact number and email address
- Details about the information requested

The PRU will not reveal the following information in response to Subject Access Requests:

- Information that might cause serious harm to the physical or mental health of the subject or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child

Subject Access Requests for all or part of the student's educational record will be provided within 15 school days.

If a Subject Access Request does not relate to the educational record, we will respond within 1 calendar month.

We reserve the right to charge for requests which are deemed to be excessive.

9. Parental Requests to see the Educational Record

Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of Subject Access rights.

For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a Subject Access Request or have given their consent. The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a Subject Access Request.

At the PRU, it is not generally the case that a pupil is either old enough or mature enough to understand their rights or the implications. Consequently, the PRU will, in most instances, grant the request from parents and provide the information. This is not a rule and a pupil's ability to understand their rights will always be judged on a case by case basis.

If parents ask for copies of information, they will be required to pay the cost of making the copies. However, the PRU is unlikely to impose a charge because of the reasons behind the referral of the pupil to the PRU, and the relationship with parents and carers.

10. Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the PRU of a change of circumstances his/her computer records will be updated as soon as is practicable.

Parents/carers are asked to provide data about their child at the start of a placement at the PRU. The parent/carers will be asked to re-check the information the PRU holds if the placement extends beyond three terms.

For Staff Data Checking Sheets will be issued every 12 months

Where a data subject challenges the accuracy of his/her data the PRU will immediately mark the record as potentially inaccurate, or “challenged”. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Management Committee under the formal Complaints Procedure.

11. CCTV

The PRU does not use CCTV on its own sites. If that changes, this policy will be updated and we will adhere to the ICO’s code of practice for the use of CCTV.

Other organisations who occupy the same location may use CCTV. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

12. Biometric recognition systems

Note that in the context of the Protection of Freedoms Act 2012, a “child” means a person under the age of 18. The PRU does not use biometric recognition systems. If this approach changes then this policy will be updated.

13. Artificial intelligence (AI)

Artificial intelligence (AI) tools are frequently available and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as Microsoft Copilot, Google Gemini and ChatGPT. The PRU recognises that AI has many uses to help pupils/students learn or staff to work more efficiently, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots. If personal and/or sensitive data is entered into an unauthorised generative AI tool, the PRU will treat this as a data breach, and will follow the adopted personal data breach procedure and consider if disciplinary steps are needed in line with its conduct policies.

14. Storage of records

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use.

- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access.
- Where personal information needs to be taken off site (in paper or electronic form), staff must have a valid reason for doing so (for example as part of the outreach support to a pupil in a school) Staff must adhere to school policies and procedures when taking data off site.
- Passwords to access school computers, online resources, laptops and other electronic devices follow the rules specified in the PRU password policy
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices. Encryption, anonymisation and pseudonymisation will be used to protect the data.
- Staff, pupils or members of the PRU Management Committee who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment.
- Members of the Management Committee are required to use PRU email addresses and use secure methods of securing and saving data.
- UK GDPR compliant cloud storage will be used for all online data storage.

15. Disposal of Records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely in line with the PRU data retention and disposal processes.

For example, we will shred or incinerate paper-based records, and override electronic files. We also use an outside company to convert paper records to electronic and to shred documents on site.

16. Data Breaches

The PRU will make all reasonable endeavours to ensure that there are no personal data breaches. If a data breach is detected the PRU will follow the procedure adopted.

All data breaches are reported to the Operations Manager (Data Protection Lead) who liaises with the appointed Data Protection Officer. When appropriate, data breaches are escalated to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website, which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

17. Training

Our staff and members of the Management Committee are provided with data protection training as part of their induction process and this is refreshed annually each year, as appropriate for their roles.

Data protection will also form part of continuing professional development, where changes to legislation or the PRU processes make it necessary to keep staff up to date.

18. Monitoring Arrangements

The EHT and Operations Manager are responsible for monitoring and reviewing this policy. The Operations Manager will check that the school complies with this policy through training, updates at team meetings and reviews of records as appropriate. This policy is reviewed annually and will also be updated if there are changes to legislation or practice.

19. Links with other policies

Where appropriate, other policies and procedure will follow the principles in this policy. For example, pupil related privacy notices are included in Inreach packs, staff induction includes GDPR responsibilities and privacy notices and the Freedom of Information policy.

20. Contact

If you would like to discuss anything in this policy, In the first instance please contact the Operations Manager or the EHT on:

Telephone: 01296 387300

The DPO can be contacted by email (dpo@turniton.co.uk)

Appendix

1. Photographs and videos

As part of the PRU activities, we may take photographs and record images of individuals within the PRU.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within the PRU on display boards and on reception monitors
- In the PRU prospectus
- Outside of PRU by external agencies such as a school photographer, newspapers, local publications

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not use any further.

2. Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member must immediately inform the Operations Manager who will work closely with the DPO, and inform the Executive Headteacher.
- The DPO (normally via the Operations Manager) will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- The Operations Manager will report the outcome of the investigation and to the link member responsible for GDPR in the Management Committee.
- The PRU's Operations Manager and DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary (actions relevant to specific data types are set out at the end of this procedure).
- The DPO will assess and advise the PRU's Operations Manager of the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO. Decisions are recorded as appropriate.

- Details of the breach and actions taken are held in the shared drives (GDPR folder)
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO, in consultation with the Operations Manager, will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will support the PRU in notifying any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The PRU will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects

- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the PRU's internal administration system.

The DPO, Operations Manager and other relevant PRU staff will review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

e.g. Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the Operations Manager as soon as they become aware of the error.
- In any cases where the recall is unsuccessful, the Operations Manager (or member of SLT) will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The Operations Manager will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The Operations Manager will liaise with the DPO throughout this process, and keep SLT colleagues and (Additional) Designated Safeguarding Lead informed, as appropriate.