



Pioneer Educational Trust  
aspire inspire

# GDPR & DATA PROTECTION POLICY

## Key document details

**Ratified:**

**Approver:**

**Next review:**

**Pending ratification**

**CEO**

## **GDPR & DATA PROTECTION POLICY**

The GDPR & Data Protection Act 2018 replaces the Data Protection Act 1998 (DPA) from 25<sup>th</sup> May 2018. This policy should be read in conjunction with GDPR & Data Protection Act 2018, the Education Pupil (Information) Regulations 2005, the School Staffing (England) Regulations 2009 (these apply to maintained schools), Independent School Standards Regulations 2010 (these apply to academies) and is based on the guidance provided by the ICO and the DfE's Data Protection Toolkit for Schools.

Pioneer Educational Trust, and the schools within its Trust intend to fully comply with the requirements of the GDPR.

Pioneer Educational Trust is the registered Data Controller with the Information Commissioner's Office (ICO) for the schools within its Trust.

### **BACKGROUND**

- The GDPR applies to staff and students and is designed to protect the rights, privacy and personal data of EU citizens.
- The definition of personal data as defined by the Regulation is ***"information relating to an identifiable natural person, whether directly or indirectly"***.
- Under the GDPR, there are stringent regulations that apply to the collection, using, disclosing, storing or disposing of personal data.
- Under the GDPR, the processing of what is termed 'special categories of personal data' has extra protections. Processing of this type of data is prohibited unless there is a requirement to do so either by law, for the safeguarding of students or to determine the working capacity of an employee. This is information that relates to race, ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences. Trusts/schools do hold special categories of personal data in their pupil and staff records where necessary.
- The Trust, the schools within the Trust and all employees working for the Trust are legally obliged to protect any information, either personal data or sensitive personal data, about pupils and staff from unauthorised access and from accidental loss or damage.
- Pioneer Educational Trust and the schools within its Trust have a duty to issue a privacy notice to staff and students on an annual basis – see appendix 2.
- Under the GDPR, any individual has the right to make a request to access the personal information about them.
- In addition, under the GDPR, the Trust and schools in its Trust may hold some information about parents and guardians.
- The Education Pupil Information Regulations 2005 cover the rights of parents to access their child's educational record.

- There is a statutory exception to the above, where parents do not have an automatic right to access defined materials under the Education (School Records) Regulations 1989. Pioneer Educational Trust will observe these statutory rights.

## **INTRODUCTION**

At Pioneer Educational Trust, we acknowledge that to function properly we need to collect and use certain types of information about staff, students and other individuals who come into contact with the Trust. We are also obliged to collect and use data to fulfil our obligations to the Education Department and other bodies. We deal with information properly in whatever way it is collected, recorded and used – on paper, electronically or any other way. We regard the lawful and correct treatment of personal information as very important to successful operations and to maintaining confidence between those with whom we deal and ourselves. We are conscious that much of the data we hold is classified as sensitive personal data and we are aware of the extra care this kind of information requires. We ensure that our organisation treats all personal information lawfully and correctly.

## **DATA PROTECTION PRINCIPLES**

All members of staff employed in our Trust are required to adhere to the six enforceable data protection principles as set out in the General Data Protection Regulation 2018.

- Data shall be processed fairly, transparently and lawfully and in particular shall not be processed unless specific conditions are met.
- Personal data shall be obtained only for one or more specified and lawful purpose and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and where necessary, kept up-to-date.
- Personal data shall not be kept for longer than is necessary for that purpose or those purposes.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

## **TRUST PRACTICE**

Within the Trust we will strictly apply the following criteria and controls. These are to:

- Notify the ICO that we process personal data and re-notify if procedures change or are amended.
- Observe fully the conditions regarding the fair collection and use of information. To achieve this we have in place and use a privacy notice, sometimes called a fair processing notice – see appendix 2.
- Meet our legal obligations to specify the purposes for which information is used.
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of information used.

- Apply strict checks to determine the length of time information is held.
- Ensure that the rights of the persons about whom information is held can be fully exercised under the Regulation. These include the right to be informed that processing is being undertaken, the right to access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information.
- Take appropriate technical and organisational security measures to safeguard personal information. We will review the physical security of buildings and storage systems as well as access to them. All portable electronic devices must be kept as securely as possible on and off school premises.
- Ensure that all Criminal Records Bureau (CRB) / Disclosure and Barring Service (DBS) records (recruitment and vetting checks) are kept in a safe central place and that no unnecessary certification information is kept longer than six months.
- Ensure that personal information is not transferred abroad without suitable safeguards.
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.
- Set out clear procedures for responding to requests for information – see appendix 1.
- Have in place secure methods for safely disposing of all electronic and paper records.
- Be sure that photographs of pupils are not included in any schools within the Trusts' publications or on the schools within the Trusts' websites without specific consent.
- Take care that CCTV that captures or processes images of identifiable individuals is done in line with the data protection principles.

We shall also ensure that:

- There is a named person with specific responsibility for data protection within the Trust.
- All persons managing and handling personal information understand that they are contractually responsible for following good data protection practice.
- All persons managing and handling personal information are trained to do so.
- Anyone wanting to make enquiries about handling personal information knows what to do.
- Anyone managing and handling personal information is appropriately supervised.
- Queries about handling personal information are properly and courteously dealt with.
- Methods of handling personal information are clearly described.
- A regular review and audit is made of the way personal information is held, managed and used.
- Methods of handling personal information are regularly assessed and evaluated.
- Performance with handling personal information is regularly assessed and evaluated.

- A breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against the members of staff concerned.
- On occasions when information is authorised for disposal, it is done appropriately.

## Appendix 1

### Subject Access Request Form

You should complete this form if you want us to supply you with a copy of any personal data we hold about you. You are currently entitled to receive this information under the Data Protection Act 1998 (DPA) and will continue to be under the EU General Data Protection Regulation (GDPR), which comes into effect on 25 May 2018. We will also provide you with information about any processing of your personal data that is being carried out, the retention periods which apply to your personal data, and any rights to rectification, erasure, or restriction of processing that may exist.

We will endeavour to respond promptly and in any event within one month of the latest of the following:

- Our receipt of your written request; or
- Our receipt of any further information we may ask you to provide to enable us to comply with your request.

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting and responding to your request. You are not obliged to complete this form to make a request, but doing so will make it easier for us to process your request quickly.

#### SECTION 1: Details of the person requesting information

Full name:	
Address:	
Contact telephone number:	
Email address:	

#### SECTION 2: Are you the data subject?

Please tick the appropriate box and read the instructions which follow it.

- YES:** I am the data subject. I enclose proof of my identity (see below).  
**(please go to section 4)**
- NO:** I am acting on behalf of the data subject. I have enclosed the data subject's written authority and proof of the data subject's identity and my own identity (see below).  
**(please go to section 3)**

To ensure we are releasing data to the right person we require you to provide us with proof of your identity and of your address. Please supply us with a photocopy or scanned image (do not send the originals) of one of both of the following:

1) Proof of Identity

Passport, photo driving licence, national identity card, birth certificate.

2) Proof of Address

Utility bill, bank statement, credit card statement (no more than 3 months old); current driving licence; current TV licence; local authority tax bill, HMRC tax document (no more than 1 year old).

If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

**SECTION 3**

**Details of the data subject** (if different from section 1)

Full name:	
School:	
Address:	
Contact telephone number:	
Email address:	

**SECTION 4: What information are you seeking?**

Please describe the information you are seeking. Please provide any relevant details you think will help us to identify the information you require.

Please note that if the information you request reveals details directly or indirectly about another person we will have to seek the consent of that person before we can let you see that information. In certain circumstances, where disclosure would adversely affect the rights and freedoms of others, we may not be able to disclose the information to you, in which case you will be informed promptly and given full reasons for that decision.

While in most cases we will be happy to provide you with copies of the information you request, we nevertheless reserve the right, in accordance with section 8(2) of the DPA, not to provide you with copies of information requested if to do so would take "disproportionate effort", or in accordance with Article 12 of the GDPR to charge a fee or refuse the request if it is considered to be "manifestly unfounded or excessive". However we will make every effort to provide you with a satisfactory form of access or summary of information if suitable.



## **SECTION 7: Declaration**

Please note that any attempt to mislead may result in prosecution.

I confirm that I have read and understood the terms of this subject access form and certify that the information given in this application to Pioneer Educational Trust is true.

I understand that it is necessary for Pioneer Educational Trust to confirm my / the data subject's identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

**Signed**.....

**Date** .....

### **Documents which must accompany this application:**

- **Evidence of your identity (see section 2)**
- **Evidence of the data subject's identity (if different from above)**
- **Authorisation from the data subject to act on their behalf (if applicable)**

**Please return the completed form to your child's school.**

### **Correcting Information**

If after you have received the information you have requested you believe that:

- Any information is inaccurate or out of date; or
- we should no longer be holding that information; or
- we are using your information for a purpose of which you were unaware;
- we may have passed inaccurate information about you to someone else;

**Then you should notify your child's school at once.**

- Any information that could cause serious harm to the physical, emotional or mental health of a pupil or another person may not be disclosed, nor should information that would reveal that the child is at risk of abuse. The same stricture applies to information relating to court proceedings.
- If there are concerns about the disclosure of information, then additional advice should be sought, usually from the Information Commission's Office.
- When redaction (blacking out or obscuring of data) has taken place, then a full copy of the information provided will be retained in order to establish, if a complaint is made, what was redacted and why.
- Information disclosed should be clear, with any codes, technical terms, abbreviations or acronyms explained. If information contained within the disclosure is difficult to read or illegible, it will be retyped.
- Information can be provided at the relevant school within the Trust with a member of staff on hand to assist if requested, or provided at face-to-face handover. The views of the applicant will be taken into account when considering the method of delivery. If postal systems have to be used, then registered or recorded mail will be used.
- Complaints will be dealt with in accordance with the Trust Complaints Procedure, which is available on-line or from the school. Should the complainant wish to take the matter further, it may be referred to the Information Commissioner [www.ico.gov.uk](http://www.ico.gov.uk).
- This policy will be reviewed by the CEO of the Trust every two years.

## Appendix 2

### Privacy Notice for Workforce

We process personal data relating to those we employ to work at, or otherwise engage to work at, our school. This is for employment purposes to assist in the running of the school or to enable individuals to be paid. The collection of this information will benefit both national and local users.

#### The categories of school information that we process include:

- personal information (such as name, employee or teacher number, national insurance number)
- special categories of data including characteristics information such as gender, age, ethnic group
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- medical information (such as food allergies or medication needed in an emergency)
- contact information (such as telephone numbers of contacts that an employee would want the school to contact in an emergency)
- address information (such as the known contact address to direct correspondence to)
- payroll information (such as bank account numbers for payment transfers)

We also process special categories of personal data that may include:

- physical or mental health needs
- racial or ethnic origin
- trade union membership
- criminal convictions data
- civil and criminal proceedings, outcomes and sentences.

This list is not exhaustive.

#### Why we collect and use workforce information

We use workforce data to:

- a) enable the development of a comprehensive picture of the workforce and how it is deployed
- b) inform the development of recruitment and retention policies
- c) enable individuals to be paid
- d) to contact you directly when you are not on the premises
- e) to contact others known to you, where you have provided their information, in cases where it would be reasonable for us to contact that individual
- f) to support the health and wellbeing of the workforce
- g) to fulfil statutory obligations as required by the Department of Education (eg the submission of the annual school workforce census)

We collect and use information under Article 6 and Article 9 of the GDPR, this enables the school to process information such as Departmental Censuses under the Education Act 1996 and other such data processes that relate education provision or payment of the individual.

#### Collecting workforce information

We collect personal information via HR/personnel forms and via the recruitment process (eg application form and new staff appointment forms)

Workforce data is essential for the school's / local authority's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

### **Storing workforce information**

We hold data securely for the set amount of time shown in our data retention schedule which is available on request.

### **Who we share workforce information with**

We routinely share this information with:

- the Department for Education (DfE)
- our HR, payroll, pensions and company benefits providers
- Pioneer Educational Trust
- our Disclosure and Barring Services Check provider

### **Why we share school workforce information**

We do not share information about our workforce members with anyone without consent unless the law and our policies allow us to do so.

We are required to share information about our school employees with the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

We are required to share information about our school employees with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

### **Requesting access to your personal data**

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact **Mrs Bhamini Lynn, PA to the Executive Leadership Team**.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>

## **Privacy Notice (How we use pupil information)**

We collect and hold personal information relating to our pupils and may also receive information about them from their previous school. The school uses and processes pupil information within the remit of the Regulation (EU) 2016/679 (General Data Protection Regulation), referred to throughout this statement as the GDPR.

### **The categories of pupil information that we process include:**

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (such as internal tests, pupils progress information and examination results)
- Medical information (such as allergies to food, medication a student may require and medical incidents that have occurred inside or outside of school that may affect learning)
- Special Educational Needs and Disabilities information (such as specific learning difficulties, specific medical needs and previous learning or medical needs)
- Behavioural information (such as rewards, achievements, sanctions and exclusions)
- Post 16 information (such as destinations data, UCAS applications and grants)
- safeguarding information (such as court orders and professional involvement)

This list is not exhaustive.

### **Why we collect and use pupil information**

We collect and use pupil information, for the following purposes:

- a) to support pupil learning
- b) to monitor and report on pupil attainment progress
- c) to provide appropriate pastoral care
- d) to assess the quality of our services
- e) to keep children safe (food allergies, or emergency contact details)
- f) to meet the statutory duties placed upon us for DfE data collections

We collect and use pupil information under Article 6 and Article 9 of the GDPR, this enables the school to process information such as assessments, special educational needs requests, Departmental Censuses under the Education Act 1996 and the Education Act 2005, examination results and other such data processes that relate educational data to the individual within the requirements for the school to provide education for the individual.

### **How we collect pupil information**

We collect pupil information via admissions and registration forms, Common Transfer Files (CTF) or secure file transfers from your previous school, pupil data collection sheets, in person, via telephone calls and/or emails initiated by the child or parent.

Pupil data is essential for the schools' operational use. Whilst the majority of pupil information you provide to us is mandatory, some of it requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this.

### **How we store pupil data**

We hold pupil data securely for the set amount of time shown in our data retention schedule which is available on request.

### **Who we share pupil information with**

We routinely share pupil information with:

- schools and other educational environments that the pupils attend after leaving us
- our local authority
- the Department for Education (DfE)
- the Police and Law Enforcement
- local School Nursing Teams
- local NHS trusts
- local Safeguarding agencies
- Pioneer Educational Trust
- our MIS, Assessment and Behaviour software providers
- Examination Boards
- Local Authorities
- Tour operators and insurance companies
- Slough Music Service
- ParentPay

### **Why we regularly share pupil information**

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

### **Requesting access to your personal data**

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact your School Office.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at

<https://ico.org.uk/concerns/>

**If you would like to discuss anything in this privacy notice, please contact your School Office.**

### **How Government uses your data**

The pupil data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures).
- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

### **Data collection requirements**

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>

### **The National Pupil Database (NPD)**

Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD).

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department.

It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>

### **Sharing by the Department**

The law allows the Department to share pupils' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the Department's NPD data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the Department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: <https://www.gov.uk/government/publications/dfе-external-data-shares>