THE PRIORY SCHOOL TRUST

# Data Protection Policy

| Trust Policy | |
|---|---|
| **Monitoring** | **Frame of engagement** |
| **Author** | |
| **Member of Staff Responsible** | Executive Principal/Data Protection Officer |
| **Consultation Parameters** | Trust Board |
| **Date of Policy** | June 2018 |
| **Review Cycle** | 2 Years |
| **Date of Review** | June 2020 |
| **Statutory Policy** | Yes |
| **Legislation** | General Data Protection Regulation (GDPR)<br>Data Protection Bill.<br>Freedom of Information Act 2000<br>Education (Pupil Information) (England) Regulations 2005 |
| **Website** | Yes |
| **Date of Website Upload** | |

| Review Table | | |
|---|---|---|
| **Date** | **Version** | **Updates** |
| June 2018 | 1 | Original |

| Contents | |
|---|---|
| **1.** | Statement of Intent |
| **2.** | Legislation and guidance |
| **3.** | Definitions |
| **4.** | The data controller |
| **5.** | Roles and responsibilities |
| **6.** | Key contact details |
| **7.** | Individual's legal duties |
| **8.** | Data protection principles |
| **9.** | Collecting personal data |
| **10.** | Sharing personal data |
| **11.** | Subject access requests and other rights of individual |
| **12.** | Parental requests to see the education record |
| **13.** | Biometric recognition systems |
| **14.** | CCTV |
| **15.** | Photographs and videos |
| **16.** | Data protection by design and default |
| **17.** | Data security and storage of records |
| **18.** | Disposal of records |
| **19.** | Personal data breaches |
| **20.** | Training |
| **21.** | Monitoring arrangements |
| **22.** | Links with other policies |
| | |

## 1. Statement of Intent

Our school is committed to the highest standards of Information Governance and protection of

individual's personal data and privacy.

We are required to keep and process relevant personal data regarding staff, pupils, their parents and guardians, governors, visitors and other individuals.

Our school aims, to ensure that all personal data is processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

All staff involved with the processing of personal data are aware of their duties and responsibilities within these guidelines. Processing may include obtaining, recording, holding, disclosing, destroying or using data. Reference to pupils in this policy includes current, past or prospective pupils.

This policy will outline how our school will comply with its legal obligations under the General Data Protection Regulation:

**2. Legislation and guidance**

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice 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.

This policy complies with our funding agreement and articles of association.

**3. Definitions**

| Term | Definition |
|---|---|
| **Personal data** | Data relating to a living individual who can be identified. |
| **Special categories of personal data** | Personal data which is more sensitive and so needs more protection, including information about an individual's:<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs |

| | |
|---|---|
| | • Trade union membership<br>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>• Physical or mental health<br>• Sexual orientation<br>• Alleged or committed offences, their proceedings and sentences. |
| **Processing** | Anything done to personal data, such as collecting, recording, holding, organising, structuring, storing, adapting, altering, retrieving, using, disclosing, disseminating, erasing or destroying.<br><br>Processing can be automated or manual. |
| **Data subject** | An individual who is the subject of personal data. |
| **Data controller** | A person or organisation that determines the purposes and the means of processing of personal data. |
| **Data processor** | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. |
| **Personal data breach** | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. |

**4. The data controller**

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school, is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

**5. Roles and responsibilities**

This policy applies to **all staff and volunteers at our** school, and to external organisations or individuals working on our behalf. Data protection is seen as a 'whole school' issue, with specific responsibilities delegated as follows:

**Data Protection Roles & Responsibilities: List of duties**

| | |
|---|---|
| Governors | • The governing board (Trustees and Local Governing Bodies) have overall responsibility for ensuring that our trust and school complies with all relevant data protection obligations. |
| Data Protection Officer (DPO) for the trust | • The DPO is responsible for overseeing the implementation of this policy, monitoring the trust's compliance with data protection law, and developing related policies and guidelines where applicable for its academy schools.<br>• They will provide an annual report of their activities directly to the trustees and, where relevant, report to the board their advice and recommendations on school data protection issues.<br>• The DPO is also the first point of contact for schools, individuals and for the ICO.<br>• Full details of the DPO's responsibilities are set out in their job description. |
| Executive Principal | • Acts as the representative of the data controller on a day-to-day basis for the trust. |
| Headteacher | • Acts as the representative of the data controller on a day-to-day basis for the school. |
| Data Protection Manager for the school. | • Is the key person with specific responsibility for Data Protection within the school and responsible for overseeing the implementation of this policy and monitoring the schools compliance with data protection law.<br>• Responsible for all information governance including data protection.<br>• Reports to the DPO and collaboratively works with the other school's Data Managers to share best practice and advice.<br>• Ensures that the school is compliant with statutory requirements in relation to personal data and privacy.<br>• Responsible for the Data Protection policy and associated procedures and embedding these into the administrative systems within school.<br>• Advises the Headteacher and Senior Leadership Team on all matters of Information Governance.<br>• Takes appropriate action for Subject Access Requests, Freedom of Information Requests, Individual Rights of data requests and Data Breach incidents.<br>• Promotes a culture of awareness and commitment to information governance and data protection throughout school, inducting and training staff.<br>• Is the main point of contact for students, staff, governors and parents who have data protection concerns.<br>• Ensures that all staff are aware of the procedures that need to be followed in the event of a data protection breach and can recognise SARs and FOI requests.<br>• Ensures that a data protection incident log is kept up to date. |

| | |
|---|---|
| IT dept | • Responsible for security of school ICT system. |
| All Staff | • Help to protect individual's personal data and privacy processing any personal data in accordance with this policy.<br>• Inform the school of any changes to their personal data<br>• Maintain an awareness of current data protection issues through training and CPD.<br>• Contact the Data Protection Manager or DPO in the following circumstances:<br>  ○ With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.<br>  ○ If they have any concerns that this policy is not being followed.<br>  ○ If they are unsure whether or not they have a lawful basis to use personal data in a particular way<br>  ○ deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area<br>  ○ To promptly pass on without delay a SAR/FOI request.<br>  ○ If there has been a data breach.<br>  ○ If they need help sharing personal data with third parties. |
| Parents | • Responsible for ensuring information that they provide to the school is accurate and up-to-date and notify us of any changes to information promptly. |

**6. Key Contact Details**

The DPO can be contacted at : dpo@tpstrust.co.uk

**7. Individual's Legal duties**

Everyone in school has a responsibility to ensure that they abide by the principles listed in this policy for handling and processing personal data and making sure that information is securely and appropriately managed. If you are unsure about the action you are taking with regard to personal data you should check with the School Data Protection Manager or DPO to ensure you are complying with the DPA.

Our School takes its duties under the Data Protection Act seriously and any member of staff found to mishandle data or share personal data with unauthorised individuals will be subject to investigation under the School's Disciplinary Policy. Deliberate, malicious or reckless breaking of the DPA will be counted as gross misconduct and could result in dismissal. Under this Act you can also be criminally liable if you knowingly or recklessly disclose personal data.

**8. Data protection principles**

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which they are processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures appropriate security of personal data

This policy sets out how the school aims to comply with these principles.

## 9. Collecting personal data

### 9.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, we rely on public interest as a basis for processing,
Whenever we first collect personal data directly from individuals, we will provide them with the School's Privacy Notice required by data protection law. Privacy Notices will remain accessible to Individuals.

### 9.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the School's Retention Schedule

**10. Sharing personal data**

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

**11. Subject access requests and other rights of individuals**

**11.1 Subject access requests**

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the School Data Protection Manager or DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

We recommend that you submit a Subject Access Request to us electronically, on our template form via the following link https://tinyurl.com/yb3dklvw which is available within the privacy notice on each school's website, but this is not compulsory.

If staff receive a subject access request they must immediately forward it to the Data Protection Manager or DPO.

**11.2 Children and subject access requests**

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Primary Schools in Trust: Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Secondary Schools in Trust: Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

**11.3 Responding to subject access requests**

We will respond to all SAR requests in line with our policy – see Appendix A

**11.4 Other data protection rights of the individual**

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it , individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the school office, Data Protection Manager or DPO. If staff receive such a request, they must immediately forward it to the school Data Protection Manager or DPO.

### 12. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil).

### 13. Biometric recognition systems.

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

### 14. CCTV

We use CCTV in various locations around some school sites to ensure they remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to dpo@tpstrust.co.uk

### 15. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

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 school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school and trust website or social media pages

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

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.

### 16. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)

- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

**17. Data security**

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

Staff will ensure that personal and sensitive data is secured in accordance with the provisions of the GDPR and the school's ICT policies or associated procedures.

**18. Disposal of records**

Personal data that is no longer needed will be disposed of securely in line with our Retention Schedule. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files.

We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

**19. Personal data breaches**

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the event of a suspected data breach, we will follow our Data Breach Procedure and where necessary report the breach to the ICO within 72 hours.

**20. Training**

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development through meeting updates and internal/external training.

### 21. Monitoring arrangements

The DPO is responsible for monitoring and updating this policy.

This policy will be reviewed **every 2 years** or updated due to legislation changes and updates as they become relevant.

### 22. Links with other policies

This data protection policy is linked to our:

- Child Protection Policy
- E-Safety/ICT policies
- ICT acceptable use policy

---

**M J Barratt**
**Executive Principal**
**The Priory School Trust**

Appendix A

SUBJECT ACCESS REQUEST POLICY

This document sets out THE PRIORY SCHOOL TRUST's policy for responding to "subject access requests" under data protection legislation.

A subject access request is a written request for personal data held about you by THE PRIORY SCHOOL TRUST. Data protection legislation gives individuals the right to know what information is held about them. However, this right is subject to certain exemptions.

When we receive a subject access request we will first check that we have enough information to be sure of your identity. This may involve us asking for 2 forms of identification or making contact via phone to confirm the request.

We will gather any manual or electronically held information (including emails) and identify any information provided by a third party or which identifies a third party. This will be redacted or removed from the record.

We will deal with your subject access request without delay and respond within one month of receipt of your request. However, if the work involved is particularly complex or if numerous requests are made then we may extend this period by up to two additional months. In this case, we will inform you about the extension and explain the reasons.

We will not charge a fee for dealing with your request unless it is manifestly unfounded or excessive. If we charge a fee, we will inform you of this and explain the reasons for doing so.

We will explain what steps have been taken in dealing with your request i.e. we will set out the source of your personal information we have gathered.

The information will be provided in a concise, transparent and easily accessible form. It may be provided in writing, or by other means, including, where appropriate, by electronic means.

There are a number of exemptions to our duty to disclose personal data. We will not disclose data that raises safeguarding concerns for a child or that is covered by legal professional privilege. We may seek legal advice in these circumstances.

If we agree that the information is inaccurate, we will correct it and where practicable, destroy the inaccurate information. If we do not agree or feel unable to decide whether the information is inaccurate, we will make a note of the alleged error and keep this on file

If you are not satisfied by our actions, you have the right to refer the matter to the Information Commissioner's Office at:

Information Commissioner's Office

Wycliffe House Water Lane Wilmslow Cheshire

SK9 5AF

If you would like to know more or have any concerns about how your personal data is being processed please contact The Data Protection Officer at: dpo@tpstrust.co.uk

Reviewed June 2018

Appendix B

FREEDOM OF INFORMATION ACT 2000

1. INTRODUCTION

From 1 January 2005 when the Freedom of Information Act 2000 (FOIA) came fully into force, there is a legal right for any person to ask an Academy for access to information that it holds. The FOI Act is overseen by the Information Commissioner who also has responsibility for GDPR, and The Environmental Information Regulations 2004.

* The Environmental Information Regulations 2004 (EIRs) enable people to access environmental information; and

* The Freedom of Information Act enables people to access all other information and the reasoning behind decisions and policies, which do not fall under DPA or EIR.

Although FOI presumes openness, it recognises the need to protect sensitive information in certain circumstances and provides for exemptions.

2. THE TRUST'S OBLIGATIONS UNDER FOIA

Academies are under a duty to provide advice and assistance to anyone requesting information. The enquirer is entitled to be told whether the Academy holds the information (the duty to confirm or deny) except where certain exemptions apply.

A well-managed records and management information system is essential to help Academy's to meet requests.

There are prescribed time limits for responding to requests for information. Requests should be dealt with within 20 days excluding Academy holidays. Wilfully concealing, damaging or destroying information in order to avoid answering an enquiry is an offence.

A valid FOI request should be in writing, state the enquirer's name and correspondence address and describe the information requested.

The academy will acknowledge receipt of the request as soon as possible detailing any costs involved and will aim to comply with the request within the statutory period (20 working days).

Any delay will be explained in writing to the person making the request.

A designated member of staff, usually the operations Manager will be responsible for ensuring requests are fulfilled within the stipulated deadline and recording details of the request on the school's tracking database.

Expressions of dissatisfaction should be handled through the Trust's existing complaints procedure.

The school will keep a record of all requests received for monitoring purposes, noting:

a) the date the request was received,

b) name and contact details of the person or organisation making the request,

c) the date the request was fulfilled or refused,

d) the reason for any exemption being applied,

e) the reason for any failure to meet the 20-day deadline.

f) any charges imposed

Reviewed June 2018