The Priestley Academy Trust

Data Protection Policy

First Version Implemented	Revision Level	Current Version Adopted by Trust	Review Date	Responsible Person
March 2017	V4.0	July 2021	July 2022	COO

Contents

Introduction

The Priestley Academy Trust (hereinafter referred to as “the Trust”) regards the lawful and correct processing of personal and sensitive data as an integral part of its purpose and vital for maintaining confidence between employees, clients and others whom we process data about, on behalf of and ourselves.

Statement of intent

The Priestley Academy Trust is required to keep and process certain information about its staff members, pupils, their families, volunteers and external contractors in accordance with its legal obligations under data protection legislation.

The Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children’s services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Trust complies with the following core principles of the UK GDPR.

Organisational methods of keeping data secure are imperative, and the Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

This Data Protection Policy explains how the Trust will meet its legal obligations concerning confidentiality and data security standards. The requirements within the policy are primarily based upon the Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR) (the Legislation) which cover data security and confidentiality of personal and sensitive personal data. (A list of important defined terms in the GDPR can be found on the back pages of this policy).

- The Trust will fully implement all aspects of the Legislation.
- The Trust will ensure all employees and others handling personal data are aware of their obligations and rights under the Legislation.
- The Trust will implement adequate and appropriate physical, technical and organisational measures to ensure the security of all data contained in or handled by those systems.

The main focus of this policy is to provide guidance about the protection, sharing and disclosure of employee and client data, but it is important to stress that maintaining confidentiality and adhering to data protection legislation applies to anyone handling personal data or sensitive (to be called "Special Category" in the GDPR) data on behalf of the Trust.

Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- The General Data Protection Regulation (UK GDPR)

- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Data Protection Act 2018
- Protection of Freedoms Act

This policy also has due regard to the following guidance:

- ICO (2018) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- DfE (2018) 'Data protection: a toolkit for schools'
- ICO (2012) 'IT asset disposal for organisations'

This policy also has due regard to The Trust's policies including, but not limited to, the following:

- Photography Policy
- Data Protection Policy
- Freedom of Information Policy
- CCTV Policy
- Child Protection and Safeguarding Policy
- Document Retention Policy
- Data Handling Procedures Policy
- Records Management Policy

Registration with the Information Commissioner

GDPR requires data controllers to register with the Information Commissioner (ICO) the categories of personal data they hold, and what they do with it.

The Trust is registered with the ICO.

The Trust is a "data controller" when it decides how to use personal data. It is a "data processor" when it is directed by a third party as to how to use personal data. Further to the GDPR both data controllers and data processors have legal obligations to safeguard personal data and are both liable if there is a breach.

Definitions of Personal Data and Sensitive Personal Data

Personal data is any personally identifiable information, so this includes:

- Employee data
- Client data
- Any other personal data processed by the Trust

Examples of personal data which the Trust processes include:

- Names, addresses, emails, telephone numbers and other contact information

- Financial information
- National Insurance numbers and payroll data
- CCTV images and photographs, video and audio recordings

Certain types of data are identified as sensitive or "special category" and attract additional legal protection. Sensitive personal data is any data that could identify a person together with information about their:

- Racial or ethnic origin
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Membership of a trade union
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence
- Information about any proceedings for any offence committed or alleged to have been committed or disposal of such proceedings or the sentence of a court in such proceedings

Data Protection Principles

We must all comply with the six Data Protection Principles that lie at the heart of the legislation. The Trust fully endorses and abides by the data protection principles. Specifically the six principles require that data is:

- **Principle 1**: processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')
- **Principle 2**: 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 shall not be considered to be incompatible with the initial purposes ('purpose limitation')
- **Principle 3**: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- **Principle 4**: 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 ('accuracy')
- **Principle 5**: 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 GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation')

- **Principle 6**: processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

Personal data and sensitive personal data must not be used other than for specific purposes. The data subject should always know that their data is being processed and the purpose. This information is provided in our Privacy Policies. When that data is sensitive, for example health information, consent is required before the data can be processed by the Trust.

All data collected from young people under the age of 16 (unless there are concerns about mental capacity in which case this should be extended), is not classed as sensitive personal data but should be treated as sensitive personal data.

A record incorporating personal data can be in computerised and/or manual form. It may include such documentation as:

- Manually stored paper data eg employee records
- Hand written notes
- Letters to and from the Trust
- Electronic records
- Printouts
- Photographs
- Videos and tape recordings

Backup data (ie archived data or disaster recovery records) is also subject to the legislation. A search in backup data should only be conducted if specifically asked for by the data subject.

Rights of Individuals

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object to processing
- Rights in relation to automated decision making and profiling

The Right of Access

The legislation gives every living person (or their authorised representative) the right to apply for access to the personal data which organisations hold about them irrespective of when and how they were compiled, ie hand written records, electronic and annual records held in a structured file, subject to certain exemptions. This is called a Subject Access Request. The legislation treats personal data relating to employees and clients alike.

Retention Periods

We store personal data on secure servers in accordance with the criteria set out in our Data Retention Policy.

Practical Implications

Understanding and complying with the principles is the key to understanding and complying with our responsibilities as a data controller. Therefore, the Trust will, through appropriate management, and strict application of criteria and controls:

- Ensure that there is a lawful basis for using personal data.
- Ensure that the use of the data is fair and will meet one of the specified conditions.
- Only process sensitive personal data where the Trust has obtained the individual's explicit consent; unless an exemption applies.
- Only process sensitive personal data, if it is absolutely necessary for the Trust to use it.
- Explain to individuals, at the time their personal data is collected, how that information will be used (within our Privacy Policies).
- Only obtain and use personal data for those purposes which are known to the individual.
- Only process personal data for the purpose for which it was given. If we need to use the data for other purposes, further consent may be needed.
- Only keep personal data that is relevant to the Trust.
- Keep personal data accurate and up to date.
- Only keep personal data for as long as is necessary (see our Retention Policy).
- Always adhere to our Subject Access Request Procedure and be receptive to any queries, requests or complaints made by individuals in connection with their personal data.
- Always allow individuals to opt-out of receiving bulk information with exception of core administrative emails such as renewals. The Trust will always suppress the details of individuals who have opted out of receiving information (e.g. marketing).
- Will always give an option to "opt in" when consent is needed to process personal data unless there is a statutory/ legal exemption.
- Take appropriate technical and organisational security measures to safeguard personal data.

In addition, the Trust will ensure that:

- There is an employee appointed as the Data Protection Officer with specific responsibility for Data Protection in the Trust (see below for roles and responsibilities).
- Everyone managing and handling personal data and sensitive personal data understands that they are legally responsible for following good data protection practice and has read and signed the Data Protection Policy.
- Everyone managing and handling personal data and sensitive personal data is appropriately supervised by their line manager.
- Enquiries about handling personal data and sensitive personal data are promptly and courteously dealt with.
- Methods of handling personal data and sensitive personal data are clearly described in polices and guidance.
- A review and audit of data protection arrangements is undertaken annually.

- Methods of handling personal data and sensitive personal data are regularly assessed and evaluated by the Data Protection Officer and relevant directors.
- Performance with personal data and sensitive personal data handling is regularly assessed and evaluated by the Data Protection Officer and relevant directors.
- Formal written data processing agreements are in place before any personal data and sensitive personal data is transferred to a third party.

Roles and Responsibilities

Maintaining confidentiality and adhering to Data Protection Legislation applies to everyone at the Trust. The Trust will take necessary steps to ensure that everyone managing and processing personal data understands that they are responsible for following good data protection practice. Employees will receive training and sign this policy every twelve months as part of their induction.

All employees (and volunteers) and sub-contractors/associates have a responsibility to:

- Observe all guidance and codes of conduct in relation to obtaining, using and disclosing personal data and sensitive personal data;
- Obtain and process personal data and sensitive personal data only for specified purposes;
- Only access personal data and sensitive personal data that is specifically required to carry out their activity or work;
- Record data correctly in both manual and electronic records;
- Ensure any personal data and sensitive personal data held is kept secure;
- Ensure that personal data and sensitive personal data is not disclosed in any form to any unauthorised third party;
- Ensure personal data and sensitive personal data is sent securely; and
- Read and sign this policy, raising any questions to check understanding.

All managers are responsible for:

- Determining if their operational area holds personal data and sensitive personal data and ensuring that the data is adequately secure, access is controlled and that the data is only used for the intended purposes(s);
- Providing clear instructions to their teams about data protection requirements and measures;
- Ensuring personal and sensitive personal data is only held for the purpose intended;
- Ensuring personal and sensitive personal data is not communicated or shared for non authorised purposes; and
- Ensuring personal and sensitive personal data is encrypted when transmitted or appropriate security measures are taken to protect when in transit or storage.

Our Data Protection Officer is Tracey Parry. Responsibilities include:

- Ensuring compliance with legislation principles;
- Progressing the Data Protection Action Plan;
- Providing guidance and advice to employees in relation to compliance with legislative requirements;
- Auditing data protection arrangements continually;

- Reporting on any breaches of Data Protection Legislation;
- In the Data Protection Officer's absence, general information can be found at http://www.ico.gov.uk/; and
- Ensuring those handling personal data are aware of their obligations by producing relevant policy, auditing the arrangements and ensuring relevant people receive training.
- Coordinating a proactive and preventative approach to data protection.
- Calculating and evaluating the risks associated with the Trust and schools' data processing.
- Having regard to the nature, scope, context and purposes of all data processing.
- Prioritising and focussing on more risky activities, e.g. where special category data is being processed.
- Promoting a culture of privacy awareness throughout the Trust community.
- Carrying out ad hoc reviews of data practices to ensure staff understand and are acting in accordance with relevant data protection laws.

The Information Commissioner's Office is responsible for overseeing compliance eg investigating complaints, issuing codes of practice and guidance, maintaining a register of data protection officers. Any failure to comply with the legislation may lead to an investigation by the ICO which could result in serious financial or other consequences for the Trust.

Breach of Policy

In the event that we fail to comply with the legislation, an individual can complain to the COO and/or ICO. We respectfully request that you notify the DPO in any event.

Dealing with a Data Breach

If a data breach is anticipated or identified, the person who identifies the actual or potential breach should immediately:

- Notify the department manager/headteacher by telephone or in person
- Notify the DPO by telephone or in person
- Upload the breach onto the GDPR system

(as the Trust may have an obligation to inform the ICO within 72 hours)

This must be done whether the breach is identified inside or outside working hours. For out of hours breach reporting contact Tracey Parry on 07772 000064.

Following notification of a breach, the Data Protection Officer will take the following actions as a matter of urgency:

- Implement a recovery plan, including damage limitations
- Assess the risks associated with the breach
- Inform the appropriate people and organisations that the breach has occurred
- Review our response and update our information security

Unlawful Processing

The legal basis for processing data will be identified and documented prior to data being processed. Under the UK GDPR, data will be lawfully processed under the following conditions.

- The consent of the data subject has been obtained.
- Processing is necessary for a contract held with the individual, or because they have asked the Trust to take specific steps before entering into a contract.
- Processing is necessary for compliance with a legal obligation (not including contractual obligations.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Processing is necessary for protecting vital interest of a data subject or another person, i.e. to protect someone's life.
- Processing is necessary for the purposes of legitimate interest pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject – this condition is not available to processing undertaken by the Trust in the performance of its tasks.

The Trust will only process personal data without consent where any of the above purposes cannot responsibly be achieved by other, less intrusive means or by processing less data.

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- Processing relates to personal data manifestly made public by the data subject
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
  - Reasons of substantial public interest with a basis in law which is proportionate to the aim pursued and which contains appropriate safeguards
  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services with a basis in law

  - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
  - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with a basis in law
- When none of the above apply, consent will be obtained by the data subject to the processing of their special category personal data.

For personal data to be processed fairly, data subjects must be made aware:

- That the personal data is being processed.
- Why the personal data is being processed.
- What the lawful basis is for that processing.
- Whether the personal data will be shared, and if so, with whom.
- The existence of the data subject's rights in relation to the processing of that personal data.
- The right of the data subject to raise a complaint with the ICO in relation to any processing.

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This may include medical emergencies where it is not possible for the data subject to give consent to the processing. In such circumstances, the DPO will be consulted and a decision made only after seeking further clarification.

Where the Trust relies on:

- 'Performance of contract' to process a child's data, the school considers the child's competence to understand what they are agreeing to, and to enter into a contract.
- 'Legitimate interests' to process a child's data, the school takes responsibility for identifying the risks and consequences of the processing, and puts age-appropriate safeguards in place.
- Consent to process a child's data, the school ensures that the requirements outlined in section 6 are met, and the school does not exploit any imbalance of power in the relationship between the school and the child.

Consent

Consent must be a positive indication expressly confirmed in words. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Consent can be withdrawn by the individual at any time.

Where consent is given, a record will be kept documenting how and when consent was given, and what the data subject was told.

The Trust ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

When pupils and staff join the school, the staff member or pupil (or, where appropriate, pupil's parent) will be required to complete a consent form for personal data use. This consent form deals with the taking and use of photographs and videos, amongst other things. Where appropriate, third parties may also be required to compete a consent form.

Where the Trust opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined above, the school obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children. In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the school on a case-by-case basis, taking into account the requirements outlined above.

Data protection by design and default

The Trust will act in accordance with the UK GDPR by adopting a data protection by design and default approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into all aspects of processing activities. In line with the data protection by default approach, the school will ensure that only data that is necessary to achieve its specific purpose will be processed.

The Trust will implement a data protection by design and default approach by using a number of methods, including, but not limited to:

- Considering data protection issues as part of the design and implementation of systems, services and practices.
- Making data protection an essential component of the core functionality of processing systems and services.
- Automatically protecting personal data in school ICT systems.
- Implementing basic technical measures within the school network and ICT systems to ensure data is kept secure.
- Promoting the identity of the COO as a point of contact.
- Ensuring that documents are written in plain language so individuals can easily understand what is being done with personal data.

Policies and Procedures

This policy should be read in conjunction with the following policies and guidance:

- Data Retention Policy
- E-Safety Policy
- The Trust Privacy Policies
- How to keep personal data safe - Staff Sheet
- Keep personal data safe - staff poster
- Keep personal data safe - staffroom poster
- Technology Acceptable Use Policy