ABBEY SCHOOLS

DATA PROTECTION POLICY

Policy Date:	December 2022
Next Review Date:	December 2023

1. Introduction

This Data Protection Policy has been produced to ensure our compliance with the Data Protection Act 2018 (DPA), GDPR and associated legislation, and it incorporates guidance from the Information Commissioner's Office (ICO).

The DPA gives individuals rights over their personal data and protects individuals from the erroneous use of their personal data.

We are registered with the ICO as a Fee Payer under registration number Z2856379.

2. Purpose

This Policy incorporates guidance from the ICO and outlines our overall approach to our responsibilities, and to individuals' rights, under the DPA 2018.

3. Scope

This Policy applies to all employees (including temporary, casual or agency staff and contractors, consultants and suppliers), third parties and others who may process personal information on our behalf. This Policy also covers any staff and students who may be involved in research or other activity that requires them to process or have access to personal data, for instance as part of a research project or as part of professional practice activities

4. Data covered by the Policy

A detailed description of this definition is available from the ICO, however, briefly, personal data is information relating to an individual where the structure of the data allows the information to be accessed i.e. as part of a relevant filing system. This includes data held manually and electronically and data compiled, stored or otherwise processed by us or by a third party on our behalf.

Special category data is personal data consisting of information relating to:

- Racial or ethnic origin
- Political opinions, Religious beliefs or other beliefs of a similar nature
- Membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- Physical or mental health or condition
- Sexual life, sexual orientation
- Biometric /genetic data

5. The Six Data Protection Principles

The DPA 2018 requires us and others who process or use any personal information on our behalf to comply with the six data protection principles.

The principles require that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- Be limited to only what is required for the purposes for which it is being collected
- Be accurate and kept up to date
- Not be kept for longer than is necessary for those purpose
- Be kept safe from unauthorised or unlawful processing and against accidental loss, destruction or damage

6. Responsibilities

We have an appointed Data Protection Officer to handle day-to-day issues which arise, and to provide us with guidance on Data Protection issues to ensure they are aware of their obligations. Our Data Protection Officer is IT Systems, and they can be contacted by dpo@itsystems.uk.net

All new members of staff will be required to complete mandatory information governance training as part of their induction and existing staff will be requested to undertake refresher training on a regular basis.

All employees are expected to:

- Familiarise themselves and comply with the six data protection principles
- Ensure any possession of personal data is necessary
- Ensure their own personal information is accurate and up to date
- Keep personal data for no longer than is necessary
- Ensure that any personal data they process is secure and in compliance with our information related policies and strategies
- Acknowledge data subjects' rights (e.g. right of access to *all* their personal data held us) under the DPA 2018, and comply with access to records
- Ensure personal data is only used for those specified purposes and is not unlawfully used for any other business Obtain consent when required for collecting, sharing or disclosing personal data

Contact the DPO at dpo@itsystems.uk.net with any concerns or doubt relating to data protection.

Students are expected comply with any security procedures implemented by us.

7. Obtaining, Disclosing and Sharing

Only personal data that is necessary for a specific school related business reason should be obtained.

Students are informed about how their data will be processed via our Privacy Notice. All staff are expected to be familiar with this document.

Data must be collected and stored in a secure manner. Personal information must not be disclosed to a third party organisation without prior consent of the individual concerned, unless the disclosure is legally required or permitted. This also includes information that would confirm whether an individual is or has been an applicant, student or employee of ours.

We may have a duty to disclose personal information to comply with legal or statutory obligation. The DPA 2018 allows the disclosure of personal data to authorised bodies, such as the police and other organisations that have a crime prevention or law enforcement function.

Personal information that is shared with third parties on a more regular basis shall be carried out under written agreement to stipulate the scope and boundaries of sharing.

8. Retention, Security and Disposal

Recipients are responsible for the processing and management of personal data needed in their roles and to ensure that the data is accurate and up-to-date

Personal information shall not be retained for longer than is necessary and shall be collected and retained only for business, regulatory or legal purposes.

In accordance with the provisions of the DPA 2018, all staff whose work involves processing personal data, whether in electronic or paper format, must take personal responsibility for its secure storage and ensure appropriate measures are in place to prevent accidental loss or destruction of, or damage to, personal data.

Staff working from home will be responsible for ensuring that personal data is stored securely and is not accessible to others.

All staff should ensure that data is destroyed in accordance with the Retention Schedule when it is no longer required.

Personal data in paper format must be shredded on site or placed in the confidential waste bins provided. Personal data must not be placed in normal, unsecure waste bins, even if torn up manually. Any member of staff found placing hard copy personal data in unsecure bins may be subject to disciplinary proceedings.

Personal data in electronic format should be securely and permanently deleted, including any metadata or backups. Staff may need to contact our IT provider for assistance when deleting electronic data as placing an electronic file in a computer recycle bin does not securely or permanently dispose of the file and further steps will be required. Those further steps will depend on the device being used and data being deleted.

Personal data stored on CDs, pen drives and other external devices which require disposal should be removed from the device securely prior to disposal. The owner of the external device is responsible for the removal of the data and the devices security. Any member of staff found using an unsecure external device to store or process personal data under our control may be subject to disciplinary.

9. Transferring Personal Data

Any transfer of personal data must be done securely in line with the our relevant policy and procedures.

Email communication is not always secure and sending personal data via external email should be avoided unless it is encrypted with a password provided to the recipient by separate means such as via telephone.

Care should be taken to ensure emails containing personal data are not sent to unintended recipients. It is important that emails are addressed correctly and care is taken when using 'reply all' or 'forwarding' or copying others in to emails. Use of the blind copy facility should be considered when sending an email to multiple recipients to avoid disclosing personal information to others.

Personal email accounts should not be used to send or receive personal data for work purpose.

10. Data Subjects Right of Access (Subject Access Requests)

Under the DPA 2018, individuals (both staff and students) have the right of access to their personal data. This applies to data held in both paper and electronic format, and within a relevant filing system.

Any individual who wishes to exercise this right should make the request through submitting a Subject Access Request Form. This is available on our website or by contacting our DPO via dpo@itsystems.uk.net

We cannot charge a fee for responding to a subject access request. We will only release any information upon receipt of the completed Subject Access Request Form, along with proof of identity or proof of authorisation where requests are made on the behalf of a data subject by a third party. The requested information will be provided within the statutory timescale of 1 month from receipt of the completed form.

For details of your other rights, please see visit the Information Commissioners (ICO) Website.

11. Reporting a Data Security Breach

We must respond to a data security breach quickly and effectively. A breach may arise from a theft, a deliberate attack on our systems, unauthorised use of personal data, accidental loss or equipment failure.

Any data breach should be reported to databreach@abbeyfed.darlington.sch.uk and the Data Protection Officer via dpo@itsystems.uk.net. In certain circumstances, breaches will also need reported to the data subject concerned.

Any breach will be investigated in line with the procedures within our Data Breach Policy. In accordance with that Policy, we will treat any breach as a serious issue. Each incident will be investigated and judged on its individual circumstances and addressed accordingly.