POLICY

For

Data Protection

Date			
September 2025			

Striving for excellence, caring for all
Within a loving and caring Christian environment.

Contents

Introduction 3
Aim 3
Scope 3
Definitions 3
The Data Protection Principles 4
School Responsibilities 4
Data Protection Roles and Responsibilities 5
Records of Processing Activity 5
Privacy Notices 5
Data Protection Impact Assessment (DPIA) 5
Security of Personal Data 5
Contracts and Information Sharing 6
Individual Rights 6
Training and Awareness 6
Surveillance Camera Systems 7
Artificial Intelligence (AI) 7
International Transfers 7
Information Commissioner's Office 7
Further Information 8
Review 8

Introduction

Abbey Academies Trust (the trust) has a statutory duty to meet its obligations as set out within data protection legislation as it processes personal data in the delivery of education.

Aim

This policy explains how the trust will meet its obligations under data protection legislation.

Scope

This policy applies to:

- All personal data processed by the trust, in any format.
- Any individual processing personal data held by the trust

Definitions

Data Protection Legislation: the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018 (“DPA 2018”), the Privacy and Electronic Communications Regulations 2003 and any other relevant law concerning the processing of personal data.

Data: information processed by automated or non-automated means, including structured files that are accessible by specific criteria

Personal data: any information that can, either directly or indirectly, identify a living person. Identifiers include name, address, date of birth, unique identification numbers (such a pupil reference numbers), postcodes, location data, online identifiers (such as IP addresses), pseudonymised data and information relating to a person's social or economic status.

Special Category Data: personal data consisting of information as to:

- Race or ethnicity,
- Political opinions,
- Religious beliefs or other beliefs of a similar nature,
- Affiliation or membership with a trade union,
- Physical or mental health or condition,
- Biometric and/or genetic data,
- Sex life or sexual orientation.

Criminal Convictions Data: personal data relating to:

- The commission or alleged commission of any offence, or
- Proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

Processing: any action on personal data, such as collection, use, storage, sharing, or destruction (whether by automated or manual means).

Data subject: the individual whose data is being processed.

Controller: the person or organisation that decides (either alone or jointly with others) how and why personal data is processed. For the purpose of this policy, the school is a controller.

Processor: any person or organisation (other than an employee of the school) that processes data on behalf of the controller.

The Data Protection Principles

The trust will adhere to the six principles of data protection, which are:

1. **Fairness, Lawfulness and Transparency**: Personal data shall be processed fairly and lawfully and in a transparent manner.
2. **Purpose Limitation**: Personal data shall be collected for specified, explicit and legitimate purposes and shall not be processed in a manner incompatible with that purpose.
3. **Data Minimisation**: Personal data shall be adequate, relevant and limited to what is necessary for the purpose.
4. **Accuracy**: Personal data shall be accurate and, where necessary, kept up to date.
5. **Storage Limitation**: Personal data shall be kept in a form that permits identification for no longer than necessary.
6. **Security**: Personal data shall be processed in a manner that ensures appropriate security.

Additionally, the trust will ensure compliance with the accountability principle, meaning we will keep records to show we're meeting these standards.

Trust Responsibilities

The trust will:

Register with the Information Commissioner's Office and pay the annual statutory data protection fee. The trust’s data protection registration number is Z2483017.
Have policies and procedures in place to support the trust’s data protection obligations.
Have staff with specific responsibility for compliance with data protection legislation.
Ensure staff processing personal data understand that they are responsible for complying with data protection legislation and are appropriately trained.

Data Protection Roles and Responsibilities

The **Trust Board** has overall responsibility for ensuring the trust operates in a manner compliant with data protection legislation and for ensuring compliance with this policy.

The **Headteacher/Head of School** has day to day responsibility for ensuring individuals are aware of, and apply, this policy.

The **Senior Leadership Team** have responsibility for supporting the Headteacher/Head of School and DPO by ensuring individuals are aware of, and apply, this policy.

The **Data Protection Officer (DPO)** will support the trust in meeting its obligations by monitoring the trust's ongoing compliance, providing advice and assistance on all data protection matters as well as acting as a single point of contact for data protection queries from individuals and the Information Commissioner's Office.

All **Trust Staff** have a responsibility to ensure they process information in line with the requirements of this policy and undertake annual data protection training.

Records of Processing Activity

The trust will maintain a record of its processing activities. The DPO will be responsible for creating and maintaining the records of processing activity in conjunction with the Trust Board, Headteacher/Head of School and Senior Leadership Team.

Privacy Notices

The trust will provide privacy notices to individuals explaining how personal data about them is used. They will be in plain English, be available upon request and be free of charge.

Data Protection Impact Assessment (DPIA)

For high-risk activities, such as large-scale processing of special category data or introducing systematic monitoring, the trust will conduct a DPIA to assess and address privacy risks. The DPO will be consulted on all DPIAs.

Security of Personal Data

The trust will implement technical and organisational controls that help reduce the risk of personal data breaches.

The trust will record and investigate all personal data breaches.

Where it is determined that a breach results in a risk to the rights and freedoms of an individual(s) the trust will aim to report the breach to the Information Commissioner's Office within 72 hours of becoming aware.

Where it is determined that a breach results in a high risk to the rights and freedoms of an individual(s) the trust will inform the individual(s) without undue delay.

Security policies and procedures will be made available to all staff.

Contracts and Information Sharing

Contracts will include measures to ensure third parties handling personal data on behalf of the trust do so in accordance with data protection legislation.

The trust will only supply personal data to third parties for the agreed purposes as set out in the contract. Third parties will not be permitted to use or disclose personal data for any other reason.

The trust will ensure that before sharing personal data with any third party, as required by contract or otherwise, appropriate security controls are in place.

The trust will ensure that information sharing arrangements are appropriately documented.

Individual Rights

The trust will have processes in place to support individuals to exercise their rights in respect of their personal data (subject to exemptions) and those processes will be clearly communicated. The trust will respond to any request within one calendar month.

The trust will consider all complaints regarding how it processes personal data. Complaints will be referred to the trust's complaints procedure in the first instance. Individuals will be made aware of their right to make a complaint to the Information Commissioner's Office and their ability to seek judicial redress.

Training and Awareness

The trust will provide mandatory annual data protection training to all staff handling personal data. Additional training will be provided where appropriate.

All staff will maintain a good awareness of data protection and the requirements of this policy.

Surveillance Camera Systems

Footage captured by Closed Circuit Television (CCTV) that identifies an individual is subject to data protection legislation.

The trust will ensure that its use of CCTV is necessary and proportionate and any introduction of CCTV for a new purpose will be subject to a Data Protection Impact Assessment prior to being used.

Wherever CCTV is in operation, the trust will display clear notices identifying the trust as the organisation responsible for the recording, the purpose for which the CCTV has been installed and contact details for further information.

CCTV recordings will be kept securely and access will be restricted only to those staff who are trained to operate the system or make decisions as to how the recordings will be used.

Artificial Intelligence (AI)

The trust is committed to using AI in a responsible, ethical and lawful manner.

No personal data will be inputted into a publicly available AI service.

Any material generated by an AI service will be checked for accuracy before being used by the trust.

Staff must not download publicly available AI services, packages or machine learning models onto trust ICT.

Any AI service procured by the trust will be subject to a DPIA before being used.

International Transfers

The trust will not transfer personal data outside of the United Kingdom, unless required by law or with appropriate safeguards in place.

Information Commissioner's Office

The trust will comply fully with all requests from the ICO to investigate and or review the trust's data processing activities.

The trust will have regard to advice and guidance produced by the ICO and will endeavour to align trust

practices to any published codes of practice.

Further Information

For further information regarding data protection within the school please contact:

Duncan Pickering, DPO
C/O Bourne Abbey C of E Primary Academy
Email: AAT.enquiries@abbeyacademies.co.uk
Tel: 01778 422163

Further information is available from the Information Commissioner's Office at www.ico.org.uk.

Review

This policy will be reviewed annually.