Abbey Academies Trust

POLICY

For

Data Protection

Amended

September 2023		

Contents

1. Introduction 2
2. Aim 2
3. Scope 2
4. Definitions 2
5. The Data Protection Principles 3
6. Trust Responsibilities 3
7. Data Protection Roles and Responsibilities 4
8. Record of Processing Activity 4
9. Privacy Notices 4
10. Data Protection Impact Assessment (DPIA) 5
11. Data security 5
12. Contracts and Information Sharing 5
13. Individual Rights 6
14. Training and Awareness 6
15. CCTV 6
16. International Transfers 6
17. Information Commissioner's Office 7
18. Further Information 7
19. Review 7
Appendix A – Lawful Bases for Processing 8

1. Introduction

Abbey Academies 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.

2. Aim

The aim of this policy is to outline the Trust's commitment and approach to its obligations as required by current data protection legislation.

3. Scope

This policy applies to:

- All personal data, regardless of format, processed by the Trust
- Any individual processing personal data held by the Trust

4. Definitions

The following definitions shall apply:

Data Protection Legislation means the General Data Protection Regulation ("GDPR"), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 and any other applicable law concerning the processing of personal data and privacy.

Data means information which:

- Is processed wholly or partly by automated means
- Is not processed by automated means and forms part of a relevant filing system i.e. a structured set of data which are accessible by specific criteria
- Is not processed by automated means and is intended to form part of a filing system

Personal data means any information, which either directly or indirectly, relates to an identified or identifiable individual. Identifiers include name, address, date of birth, unique identification numbers (such a pupil reference numbers), location data, online identifiers (such as IP addresses), pseudonymised data and information relating to a person's social or economic status.

Data subject means the person who can be identified from the information.

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

- The racial or ethnic origin of the data subject
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Affiliation with a trade union
- Physical or mental health or condition
- Biometric and/or genetic data
- Sexual life

Criminal Convictions Data means personal data concerning:

- The commission or alleged commission of any offence
- Any proceedings resulting from any offence or alleged offence committed and the resulting action

Processing in relation to information or data, means any operation(s) performed on personal data (whether automated or not) such as collection, use, storage, distribution and destruction.

Controller means a person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data is, or is to be, processed. For the purpose of this policy, the Trust is a Controller.

Processor, in relation to personal data, means any person or organisation (other than an employee of the Trust that processes data on behalf of the Controller.

5. The Data Protection Principles

The Trust shall adhere to the six principles of data protection, which are:

Principle 1: Personal data shall be processed fairly and lawfully and in a transparent manner.

Principle 2: Personal data shall be collected for specified, explicit and legitimate purposes and shall not be processed in a manner incompatible with that purpose.

Principle 3: Personal data shall be adequate, relevant and limited to what is necessary for the purpose.

Principle 4: Personal data shall be accurate and, where necessary, kept up to date.

Principle 5: Personal data shall not be kept in a form that permits identification for longer than is necessary.

Principle 6: Personal data shall be processed in a manner that ensures appropriate security.

The Trust shall ensure that it also complies with the 'accountability principle' which requires that the Trust has appropriate processes and records in place to demonstrate its compliance with the principles listed above.

6. Trust Responsibilities

The Trust shall ensure that:

- It pays the annual data protection fee to the Information Commissioner's Office. The Trust's data protection registration number is Z2483017
- It has staff in post with specific responsibility for ensuring compliance with data protection legislation

- Staff processing personal data understand that they are responsible for complying with the data protection principles and that processing activities meet a lawful basis for processing (see Appendix A)
- Staff processing data are appropriately trained to do so
- Staff are provided with appropriate data protection support and guidance

7. Data Protection Roles and Responsibilities

The following roles are in place to help the Trust achieve compliance with data protection legislation:

- The **Academy Trust** has overall responsibility for ensuring its schools operate in a manner compliant with data protection legislation and for ensuring compliance with this policy

- The **CEO/Executive Headteacher** has day to day responsibility for ensuring individuals are aware of, and apply, this policy

- The **Senior Leadership Team** have responsibility for supporting the **CEO/Executive Headteacher** 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 under data protection legislation 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 data subjects and the Information Commissioner's Office

- All **Trust Staff** have a responsibility to meet the requirements of this policy. This includes complying with individual policy requirements and undertaking training relevant to their role

8. Record of Processing Activity

The Trust shall maintain a record of its processing activities.

The DPO shall be responsible for creating and maintaining the record of processing activity in conjunction with the Academy Trust, CEO/Executive Headteacher and Senior Leadership Team.

9. Privacy Notices

The Trust shall ensure that appropriate privacy information is made available to pupils, parents/carers, staff, trustees, governors and any other data subject whose data is processed by the Trust.

Privacy notices will explain in general terms:

- The purpose for which the Trust will process the data collected

- Where the information is kept, why it is held and for how long
- Where the Trust gets personal data from and who it is shared with
- Contact details of relevant staff to allow requests for further information

Privacy notices shall be published on the schools' websites and, upon request, shall be provided in hard copy, free of charge.

10. Data Protection Impact Assessment (DPIA)

The Trust shall complete a DPIA at the early stages of any new processing activity where it is identified that high risk processing is present e.g. large scale processing, processing special category data or introducing systematic monitoring into the Trust environment.

The DPO shall be consulted on all DPIAs.

11. Data security

The Trust shall ensure it has adequate technical and organisational controls in place which aim to reduce the risk of theft, loss or unlawful processing of personal data.

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

The Trust shall record and investigate all potential 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 shall 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 shall information the individual(s) without undue delay.

12. Contracts and Information Sharing

Contracts with suppliers that deliver services on behalf of the Trust which involve the processing of personal data shall include measures to ensure personal data is handled in accordance with data protection legislation.

The Trust shall ensure that whenever personal data is shared with a third party, it is justified and necessary to meet a lawful basis for processing as set out in Appendix A to this policy.

Where necessary, the Trust shall ensure that information sharing agreements exist between the Trust and partner organisations.

The Trust shall ensure that before personal data is shared with any third party, as required by a contract or otherwise, appropriate security controls are in place.

13. Individual Rights

The Trust shall ensure that adequate processes are in place to support individuals to exercise their rights in respect of their personal data (subject to exemptions) and that those processes are clearly communicated to individuals whose data is processed by the Trust.

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

14. Training and Awareness

The Trust shall provide annual data protection training to all staff handling personal data.

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

Additional training shall be provided where appropriate.

15. CCTV

Images and audio recordings of identifiable individuals captured by Closed Circuit Television (CCTV) amount to personal data relating to that individual and will be subject to the same provisions and safeguards afforded by data protection legislation as other types of recorded information.

The Trust will ensure that its use of CCTV is necessary and proportionate to achieve its objective and any introduction of CCTV for a new purpose will be subject to a DPIA prior to being used.

Wherever CCTV is in operation, the Trust shall 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 shall be kept securely and access will be restricted only to those staff that operate the system or make decisions as to how the recordings will be used.

16. International Transfers

The Trust shall not transfer personal data outside of the European Union, to third countries or international organisations unless there is a legal requirement to do so or it can be evidenced that appropriate safeguards are in place as required by data protection legislation.

Any systematic sharing of personal data outside of the UK shall be subject to a DPIA.

17. Information Commissioner's Office

The Trust shall comply fully with all requests from the Information Commissioner's Office to investigate and/or review the Trust's data processing activities.

The Trust shall have regard to advice and guidance produced by the Information Commissioner's Office as far as it relates to the Trust's data processing activities.

The Trust shall take into account any code of practice published by the Information Commissioner's Office and shall endeavour to align its own practices accordingly.

18. Further Information

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

Duncan Pickering, Data Protection Officer
AAT.enquiries@abbeyacademies.co.uk
01778 422163

Jill Bates, Chief Operating Officer
Jill.Bates@abbeyacademies.co.uk
01778 422163

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

19. Review

This Policy shall be reviewed annually and has been approved and authorised by:

Name:	Mr Stephen Haigh
Position:	Chair of Trustees
Date:	September 2023
Due for Review by:	December 2024
Signature:	

Appendix A – Lawful Bases for Processing

In all processing activities, you must have a valid lawful basis in order to process personal data. You must determine the lawful basis before you begin processing and this must be appropriately documented.

No single basis is 'better' or more important than the others – which basis is most appropriate will depend on the purpose for processing and the school's relationship with the individuals concerned.

There are six available lawful bases for processing personal data:

1. **Consent** – freely given, informed and evidenced by a clear affirmative action.
2. **Contract** – necessary for the performance of a contract with the Data Subject (including specific steps before entering into a contract).
3. **Legal Obligation** – necessary to comply with the law.
4. **Vital Interests** – necessary to protect the life of the data subject.
5. **Public Task** – necessary to perform a task in the public interest or for the school's official functions, and the task or function has a clear basis in law.
6. **Legitimate Interests** – necessary for the school's, or a third party's, legitimate interests in circumstances where the Data Subject's right to privacy does not override those legitimate interests (NB. This legal basis is unavailable for public authorities when the processing is in connection with an official task).

If you are processing Special Category Data, you must also identify a further lawful basis. There are ten available lawful bases for processing Special Category Data:

1. **Explicit Consent** – freely given, informed and evidenced by a clear affirmative statement.
2. **Employment, social security or social protection law** – necessary to meet legal obligations in these specific areas.
3. **Vital Interests** – necessary to protect the life of the data subject or another individual where they are physically or legally incapable of giving consent.
4. **Not-for-profit Bodies** – processing carried out by a political, philosophical, religious or trade union.
5. **Deliberately made public by the Data Subject** – data that has manifestly been placed in the public domain by the Data Subject.
6. **Legal Claims** – necessary for establishing, exercising or defending legal rights.
7. **Substantial Public Interest** – necessary for reasons of substantial public interest e.g. official functions, statutory purposes, equal opportunities or preventing or detecting unlawful acts.
8. **Health and Social Care** – necessary to preventative or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, provision of health or social care or treatment or management of health and social care systems.
9. **Public interest in the area of Public Health** – such as threats to health or ensuring high standards of healthcare.
10. **Archiving Purposes** – public interest, scientific and historical research purposes or statistical purposes.

Further lawful bases are available for processing Criminal Convictions Data and advice must be sought prior to processing to determine what the appropriate lawful basis is.