GDPR Policy

Updated in September 2025

General Data Protection Regulation (GDPR) Policy

1. Introduction

Ashcroft Technology Academy (the Academy) is committed to protecting and respecting the privacy of personal data in accordance with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018. This policy outlines the way in which the Academy collects, uses, processes, and stores personal data, and the rights of individuals regarding their data.

2. Scope

This policy applies to all students (current, prospective and past), parents, guardians, employees, contractors, volunteers, and any other individuals whose personal data is collected, processed, or stored by the Academy.

3. Definitions

- **Personal Data**: Any information relating to an identified (data subject).
- **Processing**: Any operation performed on personal data, including collection, storage, use, disclosure, and deletion.
- **Data Controller**: The entity that determines the purposes and means of processing personal data.
- **Data Processor**: The entity that processes personal data on behalf of the Data Controller.

4. Data Collection

The Academy collects and processes personal data for the following purposes:

- **Educational purposes**: To provide education and related services.
- **Administrative purposes**: To manage Academy operations, including admissions, attendance, and assessment.
- **Communication**: To communicate with students, parents, and guardians about school activities, events, and updates.
- **Safety and welfare**: To ensure the safety and well-being of students and staff.
- **Legal obligations**: To comply with statutory and regulatory requirements.

5. Types of Data Collected

The types of personal data collected by the Academy may include:

- **Students**: Name, date of birth, contact details, academic records, health information, attendance records, and behavioural data.
- **Parents/Guardians**: Name, contact details, relationship to the student, and payment information.
- **Staff and Contractors**: Name, contact details, employment records, qualifications, and background checks.

6. Legal Basis for Processing

The Academy processes personal data based on one or more of the following legal bases:

- **Consent**: Where explicit consent has been obtained from the data subject.
- **Contractual necessity**: Where processing is necessary for the performance of a contract.
- **Legal obligation**: Where processing is required by law.
- **Legitimate interests**: Where processing is necessary for the legitimate interests pursued by the school, provided these interests are not overridden by the data subject's rights.

7. Data Sharing and Disclosure

The Academy will only share personal data with third parties when necessary and in accordance with GDPR. This may include:

- **Education authorities and regulatory bodies**: For compliance with legal obligations.
- **Service providers**: For the provision of services such as IT support, payment processing, and educational tools.
- **Examination bodies:** For the delivery of examinations.
- **Health and social services**: For safeguarding and welfare purposes.
- **Law enforcement agencies**: Where required by law.

8. Special category personal data

The Academy may need to share data in the event of an emergency, incident or accident, which may include details of an individual's medical condition with medical services, the police or social services.

9. Data Security

The Academy implements appropriate technical and organisational measures to protect personal data against unauthorized access, loss, or destruction. These measures include:

- **Encryption**: Protecting data in transit and at rest.
- **Access controls**: Limiting access to personal data to authorized personnel only.
- **Data minimisation**: Collecting only the data necessary for the specified purposes.
- **Network protection:** Protection from attack.

10. Data Retention

The Academy will retain personal data only for as long as necessary to fulfil the purposes for which it was collected, or as required by law. Once the data is no longer needed, it will be securely deleted as per the Academy's data retention policy.

11. Data Subject Rights

Under GDPR, data subjects have the following rights regarding their personal data:

- **Right to access**: To obtain a copy of their personal data held by the school.
- **Right to rectification**: To request correction of inaccurate or incomplete data.
- **Right to erasure**: To request the deletion of their personal data where there is no legal basis for its retention and when doing so would not conflict with the legal requirements on the Academy.
- **Right to restrict processing**: To request that processing of their data is restricted in certain circumstances.
- **Right to data portability**: To request the transfer of their data to another organisation.
- **Right to object**: To object to the processing of their data in certain circumstances.
- **Right to withdraw consent**: To withdraw consent at any time where processing is based on consent.

12. Data Breach Response

In the event of a data breach, the Academy will promptly assess the risk to data subjects and, if necessary, notify the relevant supervisory authority within 72 hours. Where the breach is likely to result in a high risk to the rights and freedoms of individuals, the affected data subjects will also be informed.

13. Data Protection Officer (DPO)

The Academy has appointed a Data Protection Officer to oversee compliance with GDPR and to act as a point of contact for data subjects.

14. Linked Policies:

The way personal data is collected, processed, or stored is aligned with the Academy safeguarding policy. The following sections of the Safeguarding Policy are especially relevant:

We have identified and assigned roles and responsibilities to manage filtering and monitoring systems. We review filtering and monitoring provision at least annually. We block harmful and inappropriate content without unreasonably impacting teaching and learning and we have effective monitoring and intervention strategies in place that meet our students' safeguarding needs. Staff should note that these systems apply to all users of ICT at the Academy. We have enhanced systems and monitoring in place to prevent cyber-attacks.