Broadway Academy Trust Policies

Our Children. Our Community. Believe it can be done!

Protection of biometric information policy

Approved by: Finance, Audit and Premises Committee

Date approved: June 2026

Next review date: June 2027

Contents

1. Introduction

1.1 This policy sets out how Broadway Academy Trust uses biometric data.

1.2 Broadway Academy Trust captures and uses individuals' biometric data in order to operate automated systems in support of the provision of education and other associated functions.

1.3 Broadway Academy Trust will take reasonable steps to ensure that members of staff will only have access to any personal data where it is necessary for them to carry out their duties and that all personal information is held securely and is not accessible to unauthorised persons.

2. Legislation and guidance

2.1 The ICO considers all biometric data to be classed as personal data, and as such it will be processed in accordance with the principles of the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR).

2.3 The use of biometric data in automated biometric recognition systems, will also be undertaken in accordance with the relevant sections of the Protection of Freedoms Act 2012.

3. Definitions

Data Breach: *a breach of security leading to data being lost or stolen, destroyed or changed without consent or accessed by someone without permission. Data breaches can be deliberate or accidental*

Data Controller: *a person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. The Academy is a data controller for the purposes of GDPR.*

Data Processor: *a person (other than an employee of the data controller), public authority, agency or any other body that processes personal data on behalf of the data controller. This applies to third party organisations who process data on behalf of the school.*

Data Protection Lead (DPL): a *nominated person with first point of contact responsibility for addressing data concerns and breaches and for liaising with the DPO*
Data Protection Officer (DPO)*: a person who is tasked with helping to protect personal data and helping an organisation to meet the GDPR compliance requirements. Ultimate accountability for compliance sits with the Governing Body and Headteacher and CEO.*

Data Subject: *an identified or identifiable living individual whose personal data is held or processed. In relation to school this includes, staff, parents, carers, students, volunteers, governors, visitors etc.*

ICO: *Information Commissioners Office (Supervising Authority in the UK)*
Personally Identifiable Information – *any information relating to an identified or identifiable, living individual.*

Personal Data – *examples of personal data include a name or title; contact details; information about behaviour and attendance; assessment and exam results; staff recruitment information and references.*

Special Categories of Personal Data – *personal data which is more sensitive and so needs more protection, including information about an individual's, racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetics; biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes, Health – physical or mental, sex life or sexual orientation. School specific data will also include information about safeguarding, pupil premium, special educational needs and disabilities, looked after children and children in need.*

Subject Access Request – *a right that a person has to obtain a copy of information held about them by the organisation*

4. Roles and responsibilities

4.1 This policy applies to all staff employed by the Academy, governors and external organisations or individuals working on its behalf. Staff who do not comply with this policy may face disciplinary action.

4.2 Governing board - has overall responsibility for ensuring that the Academy complies with all relevant data protection obligations, monitors data protection performance, ensures security measures are appropriate to keep data protected and cyber security is considered within the continuity plan.

4.3 Headteacher and CEO - acts as the representative of the data controller on a day-to-day basis.

4.4 Senior leaders - are responsible for deciding how the Academy maintains security and how data is shared, setting policies for the use of data and technology, making sure contracts with third-party processors are relevant and supporting staff with annual staff training.

4.5 Data protection officer – The Academy has appointed a suitably qualified Data Protection Officer (DPO) who is provided to the school by SIPS Education, and is contactable via gdpr@sips.co.uk or 0121 296 3000

4.6 Designated Data Protection Leads (DPLs) within the Academy act as first points of contact. The Data Protection Leads are:

Stuart Carroll, Deputy Head Teacher (student data)
Sarah Bidwell, HR Director (staff data)
David Titchener, IT Director (IT systems and data)
Parmjit Hay, Clerk to the Governors (Governors' data)

4.7 All staff - Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the relevant DPL or the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK

- If there has been a data breach or near miss
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

5. Data Protection principles and how the Academy complies as a data controller

5.1 The UK GDPR is based on data protection principles that the Academy must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

5.2 The Academy's Data Protection Policy sets out in detail how these principles are met. Key points with regards to biometric recognition systems are set out below:

Data Protection Principles	How the Academy Complies
Legality, Transparency and Fairness *Personal data will only be processed by the Academy, where it is able to demonstrate that it has a 'lawful basis' for the processing activity. Personal data will be processed fairly, and the Academy is open and honest about the uses of personal data.*	A data mapping document is a 'live' document that records all data processed by the school. A 'Lawful Basis' is recorded against each data set to evidence and record a legal reason for collecting, processing, sharing, storing, and destroying data. The Academy collects, processes and stores biometric data on the 'lawful basis' of consent. Privacy notices for students/ parents/carers, staff/volunteers, governors and visitors are available on the Academy website and paper copies can be made available from the administration office. A copy of the relevant privacy notice is also included in the Academy's admissions packs and staff induction packs.
Purpose Limitation *Personal data should be collected for specific, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.*	The Academy's data mapping document identifies the purposes for which biometric data processing takes place, a description of the categories of individuals and personal data, the categories of recipients of the data (e.g. third-party organisations). Requests for personal data disclosure outside of the stated legitimate purpose of the data collection will not be met unless they are made in the limited circumstances where there is a specific, legitimate and legally based need (e.g. through a Police WA170 form agreement).
Data Minimisation *The personal data must be 'Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'*	Data collection forms and processes will be regularly reviewed to ensure information requested is appropriate and not excessive. If a member of staff wishes to introduce the use of new technology that captures personally identifiable information, they will first speak with the data protection lead in school. The Data Protection Lead will ensure appropriate measures, including completion of a data Protection Impact assessment prior to approval of a project and identify the appropriate lawful basis. The data mapping document will be updated accordingly.

	Biometric data collected and stored is limited to that needed to manage the fingerprint and facial recognition systems – as set out in section 7 below.
Accuracy *All reasonable steps will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.*	Data is regularly checked to ensure it is as accurate as possible. Data updates are carried out when the fingerprint or facial recognition for an individual fails. Alternatives are put in place where consent is withdrawn or not given. (see section 6)
Storage Limitation *Personal data shall be kept in a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.*	Retention periods for data held in the Academy are recorded within the data mapping document The Academy uses the Information Record Management Society Toolkit to establish appropriate retention periods and data is archived and destroyed as set out in these guidelines. Personal data that is no longer required either due to it being out of date, inaccurate or in line with the school retention policy, will be disposed of securely.
Integrity and Confidential (Security) *Personal data will be processed in a manner, which 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*	The Academy expects all staff to comply with a wide range of technical and organisational measures to safeguard data; these are set out in detail in the Data Protection Policy: Biometric data safeguards include: • Use of passwords and protection of hardware • Restrictions on data sharing • Secure storage of data • Data encryption • No off-site downloading of data • Maintenance of physical security of the Academy environment to protect personal data on site
Accountability *Broadway Academy as data controller will be able to demonstrate compliance with the previous principles.*	A Data Protection Officer is appointed with suitable knowledge and experience to fulfil the role and a direct line of report through to the Head Teacher and Governing Body for data protection related matters. The Academy's Data Protection Officer is provided by SIPS Education and is contactable via gdpr@sips.co.uk or 0121 296 3000. On a day-to-day basis Data Protection Leads are the first point of contact (see section 5 for list); the relevant DPL will liaise with the Data Protection Officer for advice and guidance as required. The Academy has clear procedures in place for handling a data breach and a Subject Access Request. The DPO will undertake periodic monitoring to ensure compliance with the regulations. They must be informed of any suspected data breach and will help to investigate circumstances surrounding breaches and ascertain whether they are reportable to the ICO. The DPO will be informed by DPLs of any Subject Access Requests made to the Academy and will assist in making the response to the Data Subject.

	The Governing Body will be kept informed of ongoing compliance via reports to the Finance, Audit and Premises Committee which will include an overview of any data breaches that have occurred along with actions taken, and any Subject Access Requests received and responded to. Academy staff are GDPR trained on an annual basis via an eLearning training platform. In addition to this, regular reminders to staff on the content and expectations of this policy and the procedures to follow to safeguard personal data is carried out.. Regular Data Audits and reviews are undertaken to check the robustness of processes and systems for continued GDPR compliance.

6. Biometric recognition systems

6.1 In some instances, the Academy Trust captures and uses individuals' biometric data in order to operate automated systems.

6.2 Biometric data is personal information about an individuals' physical or behavioural characteristics that can be used to identify that person. This can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

6.3 Broadway Academy currently operates biometric systems in the following way, and for the following purpose:

- Using student fingerprints or facial recognition to access school meals as an alternative to paying with cash
- Using student fingerprints to access library service
- Using staff members' fingerprints or recognition to access school meals as an alternative to paying with cash

6.4 The ICO consider all biometric data to be classed as personal data, and as such will be processed in accordance with the principles of the General Data Protection Regulation 2018, and Data Protection Act (2018). The use of student biometric data in automated biometric recognition systems, will also be undertaken in accordance with the relevant sections of the Protection of Freedoms Act 2012.

6.5 In any situation where the Academy wishes to use students' biometric data, we will ensure that parents / carers are notified of our intention to use such data as part of an automated biometric recognition system. We will do this either before any new system is put in place, or before students first use an existing system.

6.6 Consent will be obtained from at least one parent / carer before the Academy takes any biometric data from their child and processes it. We will not process student biometric data in the following circumstances:

- If the student (verbally or in written format) objects to the use of their biometric data, or refuses to take part in the processing (irrespective of any consent given by the parent / carer)
- Where we have not received written consent from at least one parent to the processing
- Where a parent has objected in writing to the use of biometric data, even if the other parent has given written consent.

6.7 We will provide alternative ways to access relevant services where parents / carers or students have chosen not to use biometric recognition systems.

6.8 Consent can be withdrawn by parents/carers and students at any time, and in such circumstances, the Academy will ensure that any relevant data already captured is deleted.

6.9 Similarly, where the Academy wishes to use staff members' (or other adults') biometric data as part of a recognition system, we will first obtain consent to do so and before the individual takes part in the system.

If staff do not wish to have their biometric data captured, we will provide an alternative means to access the relevant service. Staff may also withdraw consent at any time, and in those instances, we will delete any relevant data already captured.

7. How biometric recognition works

7.1 In practice no actual fingerprints or scans of fingerprints or face images or scans of faces are held on Broadway Academy systems. When the biometric systems scan an individual's fingerprints or 'captures' a face for facial recognition, a mathematical formula is produced and processed. The answer to that formula is held within the system as a proxy for the fingerprint or face. This data cannot be converted back into a fingerprint by any organisation at any time.

8. Data protection lead and data protection officer

8.1 The Academy data protection lead for biometric data is David Titchener, Strategic IT Director (IT systems and data) – david.titchener@broadway-academy.co.uk

8.2 Concerns, questions or complaints can be discussed in the first instance with the Data Protection Lead or with the Academy's Data Protection Officer at gdpr@sips.co.uk or telephone number 0121 296 3000.