THE BOURNE ACADEMY

PROTECTION OF BIOMETRIC INFORMATION OF CHILDREN IN ACADEMYS

Last reviewed: Spring 2026
Next review due: Spring 2027

VISION

Our Vision is to develop literate, numerate, global citizens who ASPIRE, i.e., they are: Ambitious, Self-confident, Physically literate, Independent learners, Resilient, Emotionally literate.

AIMS

The Academy operates a cashless catering system, which students and staff have the option of accessing using biometric information. The aim of this policy is to set out the processes in place to protect biometric data collected.

LEGAL FRAMEWORK

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Protection of Freedoms Act 2012
- Data Protection Act 2018
- UK General Data Protection Regulation (GDPR)
- Department for Education (DfE) (2022) Protection of biometricinformation of children in academies and colleges

DEFINITIONS

Biometric data

Personal information about an individual's physical or behavioural characteristics that can be used to identify that person, including their fingerprints, facial shape, retina and iris patterns, and hand measurements. Currently the Academy only collects fingerprint data to allow students and staff to access their cashless catering account.

Automated biometric recognition system

A system which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to seeif there is a match in order to recognise or identify the individual.

Processing biometric data

Processing biometric data includes obtaining, recording or holding the data or carrying out any operation on the data including disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

- Recording students' biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.
- Storing students' biometric information on a database.
- Using students' biometric data as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identifyor recognise students.

Special category data

Personal data which the GDPR says is more sensitive, and so needs more protection – where biometric data is used for identification purposes, it is considered special category data.

ROLES AND RESPONSIBLITIES

Governing Body

The governing body is responsible for ensuring that this policy is compliant with statutory requirements and reviewed annually.

Principal

The Principal is responsible for ensuring the provision in this policy are implemented consistently.

Data Protection Lead (DPL)

The DPL is responsible for:

- Monitoring the Academy's compliance with data protection legislation in relation to the use of biometric data.
- Advising on when it is necessary to undertake a data protection impactassessment (DPIA) in relation to the Academy's biometric system(s). Advice can be obtained from the Academy's Data Protection Officer (DPO), SchoolPro TLC.
- Being apoint of contact for the DPO, the Information Commissioner's Office (ICO) and for individuals whose data is processed by the Academy and connected third parties.

DATA PROTECTION PRINCIPLES

The Academy processes all personal data, including biometric data, inaccordance with the key principles set out in the GDPR.

The Academy ensures biometric data is:

- Processed lawfully, fairly and in a transparent/carer manner.
- Only collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date, and that reasonable steps are taken to ensure inaccurate information is rectified or erased.
- Kept in a form which permits identification of data subjects for no longerthan is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

As the data controller, the Academy is responsible for being able to demonstrateits compliance with the provisions outlined above.

DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

Prior to processing biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out. The DPL will oversee the process of carrying out the DPIA.

The DPIA will:

- Describe the nature, scope, context and purposes of the processing.
- Assess necessity, proportionality and compliance measures.
- Identify and assess risks to individuals.
- Identify any additional measures to mitigate those risks.

When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered.

If a high risk is identified that cannot be mitigated, the DPL will consult with the DPO and the Information Commissioners Office (ICO) before the processing of the biometric data begins.

The ICO will provide the Academy with a written response (within eight weeks or 14 weeks in complex cases) advising whether the risks are acceptable, or whether the Academy needs to take further action. In some cases, the ICO may advise the Academy to not carry out the processing.

The Academy will adhere to any advice from the ICO.

NOTIFICATION AND CONSENT

Please note that the obligation to obtain consent for the processing of biometric information of children under the age of 18 is not imposed by the Data Protection Act 2018 or the GDPR. Instead, the consent requirements for biometric information is imposed by section 26 of the Protection of Freedoms Act 2012.

The following procedures will be put in place before biometric data is processed:

- Where the Academy uses students' biometric data as part of an automated biometric recognition system (e.g. using students' fingerprints to buy school meals instead of paying with cash), the Academy will comply with the requirements of the Protection of Freedoms Act 2012.
- Prior to any biometric recognition system being put in place or processing a student's biometric data, the Academy will send the student's parent/carer a Notification and Consent Form for the use of Biometric Data.
- Written consent will be sought from at least one parent/carer of the student before the Academy collects or uses a student's biometric data.

The Academy does not need to notify a particular parent/carer/carer or seek their consent if it is satisfied that:

- The parent/carer cannot be found, e.g. their whereabouts or identity is not known.
- The parent/carer lacks the mental capacity to object or consent.
- The welfare of the student requires that a particular parent/carer is not contacted,
- It is otherwise not reasonably practicable for a particular parent/carer to be notified or for their consent to be obtained.

Where neither parent/carer of a student can be notified for any of the reasons set out above, consent will be sought from the following individuals or agencies as appropriate:

- If a student is being 'looked after' by the Local Authority (LA) or is accommodated or maintained by a voluntary organisation, the LA or voluntary organisation will be notified and their written consent obtained.
- If the above does not apply, then notification will be sent to all those caring for the student and written consent will be obtained from at least one carer before the student's biometric data can be processed.

Notification sent to parent/carers and other appropriate individuals or agencies will include information regarding the following:

- Details about the type of biometric information to be taken.
- How the data will be used.
- The parent/carer's and the student's right to refuse or withdraw their consent.
- The Academy's duty to provide reasonable alternative arrangements for those students whose information cannot be processed.

The Academy will not process the biometric data of a student under the age of 18 inthe following circumstances:

- The student (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data.
- No parent/carer or carer has consented in writing to the processing.
- A parent/carer has objected in writing to such processing, even if the other parent/carer has given written consent.

Parent/carers and students can object to participation in the Academy's biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the student that has already been captured will be deleted.

Where staff members or other adults use the Academy's biometric system(s), consent will be obtained from them before they use the system.

Staff and other adults can object to taking part in the Academy's biometric system(s) and can withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted.

Alternative arrangements will be provided to any individual that does not consent to take part in the Academy's biometric system(s).

ALTERNATIVE ARRANGEMENTS

- Parent/carers, students, staff members and other relevant adults have the right to not take part in the Academy's biometric system(s).
- Where an individual objects to taking part in the Academy's biometric system(s), reasonable alternative arrangements will be provided that allow the individual to access the relevant service, e.g. where a biometric system uses student's fingerprints to pay for Academy meals, the student will be provided with a 4-digit PIN code to access their cashless catering account.
- Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service, or result in any additional burden being placed on the individual (and the student's parent/carers, where relevant).

DATA RETENTION

Biometric data will be managed and retained in line with the Academy's Data Retention Policy.

If an individual (or a student's parent/carer, where relevant) withdraws their consent for their child's biometric data to be processed, it will be deleted from the Academy's system.

BREACHES

There are appropriate and robust security measures in place to protect the biometric data held by the Academy, including using third party systems to manage and store biometric data for their particular systems.

Any breach to the Academy's biometric information will be dealt with in accordance with the Academy's Data Protection Policy and ICO requirements.

LINKS TO OTHER POLICIES

This policy has links to the following Academy policies:

- Data Protection Policy
- Retention Policy

MONITORING AND REVIEW

Governors will review this policy at every year. The policy will be promoted and implemented throughout the Academy.