Protection of Biometric Information Policy

(Students and Workforce Members)

Policy Name:	Protection of Biometric Information Policy
Version:	1
Date published:	4 6 2026
Date to be reviewed by:	June 2028
Role of Reviewer:	HR Business Partner
Statutory (Y/N):	N
Published on website: *	1A
Policy Level: **	1
Relevant to:	Staff & Students
Produced in consultation with:	COO
Approved by:	Care and Operations Committee
Approval date:	3 6 2026

*Publication on website			
Alliance website		School website	
1	Statutory publication	A	Statutory publication
2	Good practice	B	Good practice
3	Not required	C	Not required

**Policy level			
1	Trust wide	Single policy relevant to everyone and consistently applied across all schools and departments, with no variation. e.g. Complaints procedure	Statutory policies approved by the Alliance Board of Trustees (or designated Trustee Committee). Non-statutory policies approved by the CEO with exception of Executive Pay.
2	Trust core values	This policy defines the Trust core values in the form of a Trust statement to be incorporated fully into all other policies on this subject, that in addition contain relevant information, procedures and or processes contextualised to that school. e.g. Safeguarding, Behaviour	Statements in statutory policies approved by the Alliance Board of Trustees (or designated Trustee Committee). Statements in non-statutory polices approved by the CEO. Policy approved by Local School Board.
3	School/department	These policies/procedures are defined independently by schools as appropriate. E.g. Anti-bullying	Approved by Local School Board.

Contents

1. Introduction

This Policy fulfils The Alliance Schools Trust's obligation to have an appropriate policy document in place where the processing of Special Category Biometric Data takes place.

The Protection of Biometric Information Policy governs the Trust's collection, use, storage, retention and deletion of biometric data relating to students, employees, workers, volunteers, governors, contractors and other authorised users.

The nature of this processing, including what information is processed and for what purpose, is outlined in the Trust's privacy notices.

The Trust will comply with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Protection of Freedoms Act 2012
- Human Rights Act 1998
- Equality Act 2010
- Employment Rights Act 1996
- ACAS guidance relating to workplace monitoring, employee relations and fair processing of personal data
- ICO guidance on biometric data and special category data

The Trust recognises that biometric data is highly sensitive personal data and will only process such information where it is lawful, necessary, proportionate and supported by appropriate safeguards.

The Trust will comply with the additional requirements of sections 26 to 28 of the Protection of Freedoms Act 2012 relating to the use of biometric data in schools and colleges using automated biometric recognition systems.

This policy complements the Trust's Record of Processing Activities maintained under Article 30 of UK GDPR and should be read alongside:

- Data Protection Policy
- Information Security Policy
- Records Retention Schedule
- Staff Privacy Notice
- Student and Parent Privacy Notice
- Acceptable Use Policies
- CCTV Policy
- Recruitment and Employment Policies
- Disciplinary Policy

2. Scope

This policy applies to:

- All Trust employees
- Workers and agency staff
- Contractors and consultants
- Governors and Trustees

- Volunteers
- Students
- Third parties acting on behalf of the Trust

The policy applies to biometric information in all forms including:

- Hard copy records
- Electronically stored data
- Scanned images
- Cloud-based systems
- Portable devices
- Digital photographs and templates
- Communications containing biometric information

Any individual found to knowingly or recklessly breach this policy may be subject to disciplinary action, contractual sanctions and, where appropriate, referral to external authorities.

3. Definition of Biometric Data

Biometric data is defined under UK GDPR as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual.

Examples may include:

- Fingerprint recognition
- Facial recognition
- Iris or retina recognition
- Hand geometry
- Voice recognition

Biometric data is classified as Special Category Personal Data under Article 9 UK GDPR and requires enhanced protection.

An automated biometric recognition system uses technology to measure an individual's physical or behavioural characteristics using electronic equipment and compares this information against stored biometric templates in order to identify or authenticate the individual.

The Trust will wherever possible store biometric templates rather than full biometric images.

4. Definition of Processing

Processing includes obtaining, recording, storing, organising, adapting, retrieving, consulting, using, disclosing, restricting, erasing or destroying biometric data.

Examples of processing include:

a) Recording biometric data using biometric scanners or recognition systems;

b) Storing biometric templates within secure systems or databases;

c) Using biometric data to authenticate or identify an individual;

d) Deleting or securely destroying biometric records.

The Trust will only process biometric data where there is a lawful basis under Article 6 UK GDPR and a condition for processing under Article 9 UK GDPR and Schedule 1 of the Data Protection Act 2018.

The lawful basis and purpose of processing will be clearly identified within the relevant privacy notices.

5. Lawful Use of Biometric Data

Student Consent Requirements

Under the Protection of Freedoms Act 2012, schools and colleges must obtain appropriate consent before processing a student's biometric data.

The Trust will ensure that:

- Students and parents/carers are informed about the proposed use of biometric data;
- Clear privacy information is provided;
- Consent is obtained before biometric processing begins;
- Students understand they may refuse participation;
- Alternative methods are available.

The information provided will include:

- The type of biometric data collected;
- The purpose for processing;
- How the data will be stored and protected;
- Retention periods;
- Rights to refuse or withdraw consent;
- Alternative arrangements.

Where a student is considered capable of understanding the processing, their views and objections will be respected.

If a student objects or refuses to participate, their biometric data will not be processed even where parental consent has been provided.

If any parent or carer objects in writing, the Trust will not process the child's biometric data.

All consent must be:

- Freely given;
- Specific;
- Informed;
- Unambiguous;
- Recorded.

Consent will normally be obtained through written or electronic consent forms.

6. Workforce Biometric Data

The Trust recognises that the use of biometric data relating to employees and workers engages both data protection and employment law obligations.

The Trust will only process workforce biometric data where:

- There is a clear and lawful business purpose;
- Processing is necessary and proportionate;
- Less intrusive alternatives have been considered;
- Employees have been properly informed;
- Appropriate safeguards are in place.

Examples of potential lawful uses may include:

- Secure access to restricted areas;
- Authentication for safeguarding or security purposes;
- Access to systems containing sensitive information.

The Trust will not normally rely on employee consent as the sole lawful basis where there is an imbalance of power in the employment relationship.

Where biometric systems are introduced affecting staff, the Trust will:

- Carry out a Data Protection Impact Assessment (DPIA);
- Consult with staff and recognised trade unions where appropriate;
- Consider equality and discrimination impacts;
- Ensure a non-biometric alternative is available where reasonably practicable;
- Ensure staff are not unfairly disadvantaged for refusing participation.

Biometric data will not be used as the sole basis for disciplinary action or capability procedures.

Any workplace monitoring involving biometric systems will comply with:

- ACAS guidance;
- ICO Employment Practices guidance;
- UK GDPR principles;
- The Trust's disciplinary and monitoring policies.

7. Alternative Arrangements

The Trust will ensure that suitable alternatives are available for any individual who does not wish to participate in biometric processing.

Examples may include:

- PIN numbers;
- Swipe cards;
- Password access;
- Manual identification procedures.

No student, employee or other individual will be disadvantaged for refusing or withdrawing consent.

8. Data Protection Impact Assessments (DPIAs)

Before introducing any biometric system or new biometric processing activity, the Trust will complete a DPIA.

The DPIA will:

- Assess necessity and proportionality;
- Identify privacy and security risks;
- Consider impacts on rights and freedoms;
- Assess equality implications;
- Identify mitigating controls.

All DPIAs involving biometric processing must be reviewed by the Data Protection Officer (DPO) and approved by the Trust prior to implementation.

9. Data Security

The Trust will implement appropriate technical and organisational measures to protect biometric data.

Measures may include:

- Encryption;
- Access controls and permissions;
- Multi-factor authentication;
- Secure deletion methods;
- Audit logs;
- Restricted administrator access;
- Supplier due diligence.

Biometric data will only be accessible to authorised personnel with a legitimate operational need.

Any third-party supplier processing biometric data on behalf of the Trust must:

- Provide sufficient guarantees regarding data security;
- Operate under a compliant written contract;
- Process data only on documented instructions from the Trust.

10. Retention and Deletion

Biometric data will not be retained longer than necessary.

The Trust will securely delete biometric data:

- When consent is withdrawn;
- When the individual leaves the Trust;
- When the processing purpose no longer applies;
- In accordance with the Trust's retention schedule.

Secure deletion methods will be used to ensure biometric templates cannot be reconstructed or recovered.

Records of consent and withdrawal requests will also be retained in accordance with the Trust's retention requirements.

11. Data Subject Rights

Individuals whose biometric data is processed have rights under UK GDPR, including:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to object;
- Rights relating to automated decision-making.

Requests relating to biometric data should be directed to the Trust's Data Protection Officer.

12. Data Breaches

Any actual or suspected loss, unauthorised disclosure or misuse of biometric data must be reported immediately in accordance with the Trust's Data Breach Procedure.

The Trust will investigate all incidents promptly and report breaches to the Information Commission

13. Roles and Responsibilities

The Board of Trustees is responsible for:

- Ensuring compliance with legal obligations;
- Approving this policy;
- Providing oversight of biometric processing risks.

13.1. Chief Executive Officer and Senior Leaders

Senior leaders are responsible for:

- Ensuring operational compliance;
- Implementing appropriate controls;
- Ensuring staff awareness and training

13.2. Data Protection Officer

The DPO is responsible for:

- Providing advice and guidance;
- Reviewing DPIAs;
- Monitoring compliance;
- Acting as a contact point with the ICO.

13.3. Employees

All employees must:

- Comply with this policy;
- Protect biometric data appropriately;
- Report concerns or incidents promptly.

14. Policy Review

This policy will be reviewed every two years or earlier where:

- Legislation changes;
- ICO guidance changes;
- New biometric systems are introduced;
- Significant operational changes occur.

15. Contact Details

Questions regarding this policy or the Trust's use of biometric information should be directed to the Trust's Data Protection Officer.