



PRIESTNALL
SCHOOL

Protection of Biometric Information of Children in Schools

L Peet and SMBC

Date of Review: September 2026

Date of Next Review: September 2028

REVISION NUMBER	REVISION DATE	REVISION(S) MADE	REVISION APPROVAL DATE
1	Sept 26	Lawful basis section amended New sections added : — Data Security, Individual rights and Data Breaches.	September 2026

Contents Heading

INTRODUCTION.....	3
LEGAL FRAMEWORK	3
DEFINITIONS	3
BIOMETRIC DATA:	3
AUTOMATED BIOMETRIC RECOGNITION SYSTEM:	3
PROCESSING BIOMETRIC DATA:.....	3
SPECIAL CATEGORY DATA:	4
RESPONSIBILITIES.....	4
THE DATA PROTECTION ACT 2018 AND UK GDPR.....	4
DATA PROTECTION IMPACT ASSESSMENT	5
LAWFUL BASIS.....	5
OBTAINING CONSENT.....	5
ALTERNATIVE ARRANGEMENTS.....	6
DATA SECURITY	7
DATA RETENTION	7
INDIVIDUAL RIGHTS	8
DATA BREACHES	8
FURTHER INFORMATION.....	8
EQUALITY IMPACT STATEMENT	9

Introduction

Priestnall School is committed to protecting the personal data of all its students and staff. This includes any biometric data the school collects and uses. Biometric data is processed in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected. This policy outlines the procedures the school follows when collecting and processing biometric data.

Legal Framework

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

- Protection of Freedoms Act 2012 (PFA)
- Data Protection Act 2018 (DPA)
- UK General Data Protection Regulation (UK GDPR)
- DfE (2018) 'Protection of biometric information of children in schools and colleges'.

This policy should also be read in conjunction with the school's Data Protection Policy as per link below:

[Data_Protection_Policy.pdf \(laurustrust.co.uk\)](https://laurustrust.co.uk/Data_Protection_Policy.pdf)

Definitions

Biometric Data: Personal information about an individual's physical or behavioural characteristics which can be used to identify that person, such as fingerprints, facial shape, retina and iris patterns, and hand measurements.

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 see if there is a match in order to recognise or identify the individual.

Processing biometric data: Processing of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

- recording student biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
- storing student biometric information on a database system; or

- using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise students.

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

Responsibilities

The Head of School is responsible for ensuring the provisions of this policy are implemented throughout the school and ensuring any risks associated with the processing of biometric data are identified and mitigated.

Staff are responsible for recognising the use of biometric data and ensuring appropriate advice is requested from the Trust Director of Assessment, Accreditation and Compliance to ensure any processing is fair and legal.

The Data Protection Act 2018 and UK GDPR

As data controllers, schools must process student personal data (which includes biometric data), in accordance with the UK GDPR / Data Protection Act 2018 (DPA). The provisions in the Protection of Freedoms Act 2012 are in addition to the requirements under the DPA with which schools must continue to comply.

The DPA sets out key data protection principles with which all data controllers must comply. This ensures data is:

- Processed lawfully, fairly and in a transparent 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 longer than 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 school is responsible for being able to demonstrate its compliance with the provisions outlined above.

Data Protection Impact Assessment

The Data Protection Act 2018 requires an organisation to ensure a Data Protection Impact Assessment (DPIA) is carried out for any high-risk processing.

The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks during the design stages of a process and throughout the lifecycle of the initiative. Prior to any new processing of biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out.

The school's DPO will oversee and monitor the process of carrying out the DPIA.

Lawful Basis

Biometric data constitutes as special category data and the processing of such data is subject to the requirements of the UK General Data Protection Regulations (GDPR). Before processing biometric data for the purpose of uniquely identifying an individual, the school will identify and document an appropriate lawful basis under Article 6 UK GDPR and a separate condition under Article 9 UK GDPR. Where the school relies on consent, the consent must meet the applicable UK GDPR standard and, for special category biometric data, must be explicit.

To comply with these regulations Priestnall School obtain parent/carer consent so that we may process biometric data. Where a student is aged 12 or over, the school will also obtain the student's consent.

Obtaining consent

Alongside data protection legislation, there is also an obligation to obtain consent for the processing of biometric information of children under the age of 18, under provisions in Section 26 of the Protection of Freedoms Act 2012.

Priestnall School will notify each parent/carer of a student under the age of 18 if it is to use the student's biometric data as part of an automated biometric recognition system.

As long as student or a parent/carer does not object, the written consent of only one parent/carer is required for a school to process the child's biometric information. A

student does not have to object in writing but a parent's objection must be written.

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

- the parent/carer cannot be found, for example, his or her whereabouts or identity is not known;
- the parent/carer lacks the mental capacity to object or to consent;
- the welfare of the student requires that a particular parent/carer is not contacted, for example where a student has been separated from an abusive parent/carer who is not to be informed of the student's whereabouts; or
- where it is otherwise not reasonably practicable for a particular parent/carer to be notified or for his or her consent to be obtained.

Where neither of the parent/carers of a student can be notified for one of the reasons set out above, consent will be sought from one of the following (as set out by section 27 of the Protection of Freedoms Act 2012):

- if the student is being 'looked after' by a local authority or is accommodated or maintained by a voluntary organisation the local authority, 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 must be gained from at least one
- carer before the students' biometric data can be processed.

Notification sent to parents/carers will outline the following information about the processing of the student's biometric information to ensure that parents/carers are fully informed about what is being proposed. This includes:

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

Alternative Arrangements

Parents, carers, students, staff members and other relevant adults have the right to not take part in the school's biometric system(s). Where an objection is received the school

will put in reasonable alternative arrangements to ensure the individual is able to access the relevant service, e.g. where a biometric system uses student fingerprints to pay for school meals, the student will be provided with a lunch card.

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 parents/carers, where relevant).

Data Security

The school recognises that biometric data is sensitive personal information and will implement appropriate technical and organisational measures to protect it from unauthorised access, loss, misuse, alteration or disclosure.

Access to biometric data and systems will be restricted to authorised staff who require access as part of their role. Appropriate access controls, including role-based permissions and multi-factor authentication for administrative accounts where available, will be implemented. Access to biometric systems will be monitored through audit logs and subject to periodic review.

Where third-party suppliers are used to provide or support biometric systems, the school will ensure appropriate contractual, technical and organisational safeguards are in place.

Supplier access, including remote support access, will be limited to authorised activities and appropriately monitored.

Any actual or suspected loss, unauthorised access, disclosure or misuse of biometric data will be managed in accordance with the school's Personal Data Breach Procedure.

Data Retention

Biometric data will be managed and retained in line with the school's Records Retention Schedule. For more information, please contact dataprotection@laurustrust.co.uk.

If consent for biometric data processing is withdrawn by the individual or their parent/carer, the data will be deleted from the relevant system, no more than 72 hours after the consent is withdrawn.

Once a student or staff member leaves, the biometric data will be deleted from the school's system no more than 72 hours later.

Individual rights

Individuals have a number of rights under data protection legislation, including the right to request access to their personal data, request the correction of inaccurate information, request the deletion or restriction of processing in certain circumstances, and withdraw consent where consent is relied upon. Requests relating to biometric data will be handled in accordance with the school's Data Subject Rights Guidance and Procedure. Individuals also have the right to raise concerns with the school and, if dissatisfied, to complain to the Information Commissioner's Office (ICO).

Data Breaches

Any actual or suspected personal data breach involving biometric information must be reported immediately in accordance with the school's Personal Data Breach Policy. The school will investigate all incidents, take appropriate steps to contain and mitigate any risks, and assess whether the breach must be reported to the Information Commissioner's Office (ICO) and/or affected individuals in line with data protection legislation. Where necessary, lessons learned from incidents will be used to improve security controls, procedures and staff awareness.

Further Information

Department for Education's 'Protection of Biometric Information of Children in schools – Advice for proprietors, governing bodies, head teachers, principals and school staff: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1092507/Biometrics_Guidance_July_2022.pdf

ICO guidance on data protection for education establishments: <https://ico.org.uk/your-data-matters/schools/>

Equality Impact Statement

Names and title of people involved with this assessment	Rachel Robinson Trust Director of Inclusion
Impact assessment carried out with regard to identified characteristics	☒ Race ☒ Disability ☒ Sex ☒ Age ☒ Religious Belief ☒ Sexual orientation ☒ Gender Reassignment
Summary of any issue/proposed changes	n/a
Date	14.09.26
Date of next review	September 2028



PRIESTNALL
SCHOOL

Priestnall School
Priestnall Road
Heaton Mersey
Stockport
SK4 3HP

t: 0161 549 7300
e: enquiries@priestnallschool.org.uk
w: www.priestnallschool.org.uk