

Greenshaw Learning Trust

Biometric Data Usage Procedure

Greenshaw Learning Trust

Biometric Data Usage Procedure

Contents

PART A	3
1.1. Application	3
1.2. Approval and review	3
1.3. Terminology	3
1.4. Responsibilities	4
1.5. Associated policies and procedures	4
PART B	5
2. Introduction	5
3. Purpose of Biometrics	5
4. Consent and Withdrawal of Consent	5
5. Storage of Biometric data	6
6. Retention of Biometric data	6

PART A

1.1. Application

This Greenshaw Learning Trust Procedure applies to the Greenshaw Learning Trust as a whole and to all the schools and service units in the Trust, in accordance with and pursuant to the Data Protection Policy of the Greenshaw Learning Trust.

The Greenshaw Learning Trust, including all the schools and services within the Trust, their Trustees, governors and staff, must abide by this Procedure.

This Procedure must be read in conjunction with the GLT Data Protection Policy; all the terms of the GLT Data Protection Policy apply to the interpretation and implementation of this Procedure; if there is any ambiguity or conflict the GLT Data Protection Policy must be followed.

In implementing this Procedure the Trust and its schools and staff, must take account of any advice or instruction given to them by the GLT Data Protection Officer, the GLT CEO or Board of Trustees.

If there is any question or doubt about the interpretation or implementation of this Procedure, the GLT Data Protection Officer or GLT CEO should be consulted.

1.2. Approval and review:

Maintenance of this Procedure is the responsibility of the GLT CEO.

This Procedure was approved by the Board of Trustees on: 16 December 2022.

This Procedure is due for review by: 28 February 2025.

1.3. Terminology

The Trust means the Greenshaw Learning Trust (GLT).

- School means a school within the Greenshaw Learning Trust.
- Headteacher means the headteacher or principal of the school.
- CEO means the chief executive officer of the Greenshaw Learning Trust.
- Governing Body means the committee of the Board of Trustees to which Trustees have delegated appropriate powers and functions relating to the governance of the school.
- GLT Data Protection Officer means SchoolPro TLC.
- School Data Protection Lead means the point of contact for data protection matters for staff, students and parents in the school.

References in this Procedure to a school in the Trust should also be read as the Trust Shared Service for services, functions and staff of the Trust that are not contained within a school budget and/or are not the responsibility of a Headteacher and/or Governing Body. With respect to the Trust Shared

Service, references in this Procedure to the responsibilities of the Headteacher and Governing Body should be read as the GLT CEO and the GLT Board of Trustees respectively.

1.4. Responsibilities

For the purposes of data protection legislation, the Greenshaw Learning Trust is the Data Controller, and can be contacted by writing to Greenshaw Learning Trust, ORU Sutton, Throwley Way, Sutton, SM1 4AF.

The GLT Data Protection Officer is: SchoolPro TLC

Email: DPO@schoolpro.uk

Address: Unit 1b Aerotech Business Park, Bamfurlong

Lane, Cheltenham, United Kingdom, GL51 6TU

Telephone: 01452 947633

Lead Contact: Ben Craig

1.5. Associated policies and procedures

This Procedure is a constituent part of the GLT Data Protection Policy.

The following Trust policies and procedures are directly related to and complement this GLT Biometric Data Usage Procedure:

- GLT Safeguarding Policy and associated school policies and addendums.

PART B

2. Introduction

Biometric data means personal information about an individual's 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.

The Greenshaw Learning Trust recognises that biometrics systems can be privacy intrusive.

The Greenshaw Learning Trust does not currently make use of facial recognition data.

All biometric data is considered to be special category data under the UK General Data Protection Regulation (UK GDPR). This means the data is more sensitive and requires more protection as this type of data could create more significant risks to a person's fundamental rights and freedoms.

This Procedure complies with The Protection of Freedoms Act 2012 (sections 26 to 28), the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR) and the guidance produced by the Information Commissioner.

The purpose of this Procedure is to regulate the management, operation and use of biometric data across the Trust.

An automated biometric recognition system uses technology 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' of biometric data 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.

As biometric data is special category data, in order to lawfully process this data, the Trust must have a legal basis for processing personal data and a separate explicit consent (which satisfies the fair processing conditions for personal data and special category data).

3. Purpose of Biometric Data

The Greenshaw Learning Trust collects and uses biometric data individuals in order to provide education and associated functions, including for the following purposes:

- To enable the efficient operation of school canteen provision.
- To enable the efficient operation of a school library.

4. Consent and Withdrawal of Consent

In accordance with the Data Protection Policy, each school will notify staff, students and parents of how the school intends to use and process biometric data and seek their consent.

If a member of staff, student or parent objects to the processing of their biometric data, the school will not be permitted to use the biometric data and will provide reasonable alternatives which will allow the student or staff member to access the same facilities that they would have had access to had their biometric data been used.

Staff, students and parents can also object at a later stage to the use of their biometric data. This should be in writing or by email to the School Data Protection Lead, requesting that the school no longer uses the biometric data.

5. Storage of Biometric Data

Biometric data will be kept securely and systems will be put in place to prevent any unauthorised or unlawful access/use in accordance with the GLT Data Protection Policy.

The biometric data will only be used for the purposes for which it was obtained and such data will not be unlawfully disclosed to third parties.

6. Retention of Biometric Data

In accordance with the GLT Data Retention Procedure, biometric data will be stored by the school or by the Third-Party provider (as specified in the school or Trust Privacy Notice) for as long as consent is provided.

If consent has been withdrawn, or once a student or staff member leaves, the biometric data will be deleted from the system within 72 hours.