Claverley CE Primary school

Protection of Biometric Data Policy

Date policy last reviewed: Nov 2022

Contents:

Statement of intent

Claverley CE Primary School is committed to protecting the personal data of all its pupils and staff; this includes any biometric data we collect and process.

We collect and process biometric data in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected. We will treat the data collected with appropriate care.

This policy outlines the procedure the school follows when collecting and processing biometric data.

1. Legal framework

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

- Protection of Freedoms Act 2012
- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- DfE (2022) 'Protection of biometric information of children in schools and colleges'
- DfE (2018) 'Data protection: a toolkit for schools'

This policy operates in conjunction with the following school policies:

- Data Protection Policy
- Records Management Policy
- Data and Cyber-security Breach Prevention and Management Plan

2. Definitions

"**Biometric data**" is personal information, resulting from specific technical processing, 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, hand measurements, and voice. All biometric data is personal data.

An "**automated biometric recognition system**" is 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. Biometric recognition systems can use many kinds of physical or behavioural characteristics, such as those listed above.

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

"**Special category data**" is personal data which the UK GDPR says is more sensitive, and so needs more protection. Where biometric data is used for identification purposes, e.g. through keystroke analysis, it is considered special category data.

3. Roles and responsibilities

The governing body is responsible for reviewing this policy on an annual basis.

The headteacher is responsible for ensuring the provisions in this policy are implemented consistently.

The DPO is responsible for:

- Monitoring the school's compliance with data protection legislation in relation to the use of biometric data.
- Identifying the additional risks associated with using automated biometric technology by conducting a data protection impact assessment (DPIA).
- Being the first point of contact for the ICO and for individuals whose data is processed by the school and connected third parties.

4. Data protection principles

The school processes all personal data, including biometric data, in accordance with the key principles set out in the UK GDPR. The school ensures biometric 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.

5. 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 DPO will oversee and monitor 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.
- Be reviewed frequently and kept updated.

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 DPO will consult the ICO before the processing of the biometric data begins.

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

6. Notification and consent

Parents are informed that the school uses a system called 'Junior Librarian' to enable children to withdraw books from the school library. It is a biometric system where pupils can use a fingerprint to loan a book. In line with GDPR, parents must give permission for their child to use the system.

Please note: 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 UK GDPR. Instead, the consent requirements for biometric information are imposed by section 26 of the Protection of Freedoms Act 2012.

Where the school uses pupils' biometric data as part of an automated biometric recognition system (e.g. using pupils' fingerprints to borrow a book from the library), the school will comply with the requirements of the Protection of Freedoms Act 2012.

Prior to any biometric recognition system being put in place or processing pupils' biometric data, the school will send pupils' parents a consent letter prior to the child starting the school. Written consent will be sought from at least one parent of the pupil before the school collects or uses a pupil's biometric data.

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

Notification sent to parents 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
- How the data will be stored
- The parent's and the pupil's right to refuse or withdraw their consent
- The school's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed

The school will not process the biometric data of a pupil under the age of 18 in the following circumstances:

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

7. Storage and data retention

School uses a registered company and is therefore GDPR compliant. On registering a fingerprint, the system converts 5-points on the finger into a long string and stores the fingerprint data in an encrypted file. The 5-point string cannot be used in any other system and it would only ever be possible to recreate a partial fingerprint image. When a child leaves the school, the fingerprint data is deleted from the system.

8. Security and breaches

The outcome of the DPIA will be used to identify the security measures that will be put in place to protect any unlawful and/or unauthorised access to the biometric data stored by the school.

These security measures and the process that will be followed if there is a breach to the school's biometric systems are outlined in the school's Data and Cyber-security Breach Prevention and Management Plan.

9. Monitoring and review

The governing board will review this policy on an annual basis. The next scheduled review date for this policy is Nov 2023.