Three Spires TRUST

*'Life in all its fullness'*

# Protection of Biometric Data Policy

| | |
|---|---|
| Policy owner | Director of Operations / ICT Business Partner |
| Approved by | Trust Board |
| Approval date | Summer 2024 |
| Review date | Summer 2025 |

**Policy Version Control**

| Version | Date | Author | Changes |
|---|---|---|---|
| 1.0 | August 2024 | CL | Original policy |
| | | | |
| | | | |
| | | | |

**Contents:**

**Statement of Intent**
Three Spires Trust 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, and ensure the processing is necessary and proportionate.

This policy outlines the procedure the trust 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 academies and colleges
- DfE (2023) 'Data protection in schools'

This policy operates in conjunction with the following policies:

- Data Protection Policy
- Records Management Policy
- ICT Security Policy

## 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 Trust board is responsible for reviewing this policy on a bi-annual basis.

The Director of Operations is responsible for ensuring the provisions in this policy are implemented consistently.

The ICT Business Partner will be responsible for:

- Ensuring data protection performance is monitored regularly.
- Providing support to the DPO, as necessary.
- Ensuring effective network security infrastructure is in place to keep personal data protected.
- Reviewing this policy on an annual basis.

The Business Manager at each academy will be responsible for:

- Ensuring the provisions in this policy are implemented consistently.
- Ensuring staff receive appropriate training on data protection annually.
- Deciding on how the school processes and uses biometric data.

The DPO will be 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 trust and our academies will process all personal data, including biometric data, in accordance with the key principles set out in the UK GDPR. The school will ensure 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 trust and our academies will be responsible for being able to demonstrate its compliance with the provisions outlined above.

Information will be included in the trust privacy notices explaining how biometric data is to be processed and stored, including the rights available to individuals in respect of the processing.

## 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 academy 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.

Each DPIA will be treated as a 'living' document to help manage and review the risks of the processing of the biometric data and the measures put in place on an ongoing basis. DPIAs will be reviewed annually or in response to any changes.

## 6. Notification and consent

Consent requirements for biometric information are imposed by section 26 of the Protection of Freedoms Act 2012.

Where the trust uses pupils' biometric data as part of an automated biometric recognition system (e.g. using pupils' fingerprints to receive school dinners instead of paying with cash), the trust 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 trust will send pupils' parents a Parental Notification and Consent Form for the use of Biometric Data. Written consent will be sought from at least one parent of the pupil before the trust collects or uses a pupil's biometric data.

The name and contact details of pupils' parents will be taken from the local academy admission register. Where the name of only one parent is included on the admissions register, the Principal will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent.

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

- The parent cannot be found, e.g. their whereabouts or identity is not known.
- The parent lacks the mental capacity to object or consent.
- The welfare of the pupil requires that a particular parent is not contacted, e.g. where a pupil has been separated from an abusive parent who must not be informed of the pupil's whereabouts.
- It is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.

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:

- If a pupil is being 'looked after' by the 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 pupil and written consent will be obtained from at least one carer before the pupil's biometric data can be processed.

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 academies duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed

The trust 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

Parents and pupils will be made aware that they can object to participation in the trust biometric systems or withdraw their consent at any time, and that if they do this, the trust or academy will provide them with an alternative method of accessing the relevant services. Pupils will be informed that they can object or refuse to allow their biometric data to be collected and used via letter. The steps taken by the trust and our academies to inform pupils will take account of their age and level of understanding. Parents will also be informed of their child's right to object and will be encouraged to discuss this with their child.

Where a pupil or their parents object, any biometric data relating to the pupil that has already been captured will be deleted. If a pupil objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the trust will ensure that the pupil's

biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the pupil's parent.

Where staff members or other adults use the academies biometric systems, consent will be obtained from them before they use the system. Staff and other adults can object to taking part in the trusts biometric systems 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 trusts biometric systems, in line with the Alternative arrangements section of this policy.

## 7. Alternative arrangements

Parents, pupils, staff members and other relevant adults have the right to not take part in the trusts biometric systems.

Where an individual objects to taking part in the trusts biometric systems, reasonable alternative arrangements will be provided that allow the individual to access the relevant service, e.g. where a biometric system uses pupil's fingerprints to pay for meals, the pupil will be able to use cash for the transaction instead.

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 or the pupil's parents, where relevant.

## 8. Storage and data retention

Biometric data will be managed and retained in line with the trust Records Management Policy.

The trust will only store and process biometric information for the purpose for which it was originally obtained and consent provides.

If an individual, including a pupil's parent, where relevant, withdraws their consent for their or their child's biometric data to be processed, it will be erased from the academy system.

## 9. 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 trust.

Biometric data will not be unlawfully disclosed to third parties.

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 trusts ICT security Policy.

## 10. Monitoring and review

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

Any changes made to this policy will be communicated to all staff, parents and pupils.