TANFIELD
SCHOOL

HARD WORK | TRUST | FAIRNESS

Protection of Biometric Data Policy

Document Control

Document reference:	Protection of Biometric Information	**Date implemented:**	April 2024
Version:	1.0	**Date modified:**	April 2024
Revision due date:	April 2025		
Reviewed by:	Matthew Pearson (IT & Electrical Manager)	**Sign and date:**	June 2024
Authorised by:	Christine Hewitson (Director of Business & Finance)	**Sign and date:**	June 2024

Change History

Version	Date	Description
1.0	April 2024	Initial draft, start of document

Related Documents/Policies

References	Title
	Data Protection Policy
	Data Retention Schedule
	Data Breach Procedure
	Data Protection Act 2018
	UK GDPR
	Protection of Freedoms Act 2012

Contents

1. Statement of intent

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

2. Legal framework

2.1 Legislation and guidance

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

- Data Protection Act 2018
- UK General Data Protection Regulations (UK GDPR)
- Protection of Freedoms Act 2012
- DfE 'Protection of biometric data of children in schools and colleges' July 2022

2.2 School policies and procedures

This policy operates in conjunction with the following school policies and procedures:

- Data Protection Policy
- Data Retention Schedule
- Data Breach Procedure

3. Definitions

- **Biometric data -** Personal information 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, 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 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** – 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.

4. 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 data protection officer (DPO) is responsible for:

- Monitoring the school's compliance with data protection legislation in relation to the use of biometric data.
- Advising on when it is necessary to undertake a data protection impact assessment (DPIA) in relation to the school's biometric system(s).
- Being the first point of contact for the ICO and for individuals whose data is processed by the school and connected third parties.

5. Data protection principles

The school processes all personal data, including biometric data, in accordance with the six Data Protection Principles set out in in the UK GDPR.

The school ensures that 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.

6. Data protection impact assessments (DPIAs)

Prior to processing biometric data or implementing a system that involves the processing of biometric data, or any other special category 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

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 with the ICO before processing of the biometric data begins.

The ICO will provide the school with a written response (within eight weeks or fourteen 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 given by the ICO.

7. Notification and consent

Please note that obligation to gain 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, consent requirements for biometric information is imposed by section 26 of the Protection of Freedoms Act 2012.

Where the school use biometric information as part of an automated biometric recognition system (e.g. using pupils' fingerprints to receive school dinners instead of paying with cash), 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 a pupil's biometric data, the school will send the pupil's parents a consent form for the use of biometric data or request consent via appropriate digital systems. Consent will be sought from at least one parent of the pupil before the school collects or uses a pupil's biometric data.

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

The school 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
- The parent's and 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 biometric data of a pupil 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 to the processing
- A parent has objected to the processing, even if another parent has given consent

Parents and pupils can object to participation in the school's biometric system(s) or withdraw their consent at any time. Where this happens, 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 school 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(s).

Pupils will be informed that they can object or refuse to allow their biometric data to be collected and used via a consent form.

Where staff members or other adults use the school's biometric system(s), consent will be obtained from them before they use the system.

Staff and other adults can object to taking part in the school's biometric system(s) 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 school's biometric system(s), in line with section 8 of this policy.

8. Alternative arrangements

Parents, pupils, staff members and other relevant adults have the right to not take part in the school's biometric system(s).

Where an individual objects to taking part in the school's biometric system(s), 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 school meals, the pupil will be able to use a unique PIN number 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 (and the pupil's parents, where relevant).

9. Data retention

Biometric data will be managed and retained in line with the school's data retention schedule.

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

10. Data breaches

There are appropriate and robust security measures in place to protect the biometric data held by the school.

Any breach to the school's biometric system(s) will be dealt with in accordance with the data breach procedure.

11. Monitoring and review

The governing board will review this policy on an annual basis. Any changes made to this policy will be communicated to all staff, parents and pupils. A copy of this policy is available on our school website. Paper copies can also be provided upon request to the school office.

Appendix: Notification template for the use of biometric data

Dear parent/carer

Tanfield School wishes to use information about your child as part of our new electronically-operated recognition system.

The information from your child that we wish to use is referred to as 'biometric information'. Under the Protection of Freedoms Act 2012 (sections 26 to 28), we are required to notify each parent of a child and obtain the online consent of at least one parent.

Biometric information and how it will be used

Biometric information is information about a person's characteristics that can be used to identify them, for example, information from their fingerprint. We would like to take and use information from your child's biometric and use this information for the purpose of providing your child with food and drinks during break and lunch periods.

You should note that the law places specific requirements on schools and colleges when using personal information, such as biometric information, about students for the purposes of an automated biometric recognition system.

For example:

(a) We cannot use the information for any purpose other than those for which it was originally obtained and made known to the parent(s) (i.e. as stated above);

(b) We must ensure that the information is stored securely;

(c) We must tell you what we intend to do with the information;

(d) Unless the law allows it, we cannot disclose personal information to another person/body – you should note that the only person/body that we wish to share the information with is Live Register Ltd. This is necessary in order to support and maintain the system.

Providing your consent/objecting

You can object to the proposed processing of your child's biometric information at a later stage or withdraw any consent you have previously given. This means that, if you give consent but later change your mind, you can withdraw this consent. Please note that any consent, withdrawal of consent or objection from a parent must be in writing.

We are happy to answer any questions you or your child may have.

If you do not wish your child's biometric information to be processed by Tanfield School, or your child objects to such processing, we will look to provide reasonable alternative arrangements for children who are not going to use the automated system.

To give consent for the processing of your child's biometric information, please do so via Arbor.

Please note that when your child leaves Tanfield School, or if for some other reason he/she ceases to use the biometric system, his/her biometric data will be securely deleted.

By giving consent, you are authorising Tanfield School to use your child's biometric information as set out above.

Yours faithfully

Christine Hewitson

Director of Finance and Operations