Protection of Biometric Data Policy

Date policy last reviewed: _____

Signed by:

_____	CEO	Date:	_____
_____	Chair of governors	Date:	_____

Last Updated: September 2023

Contents:

Statement of intent

Aspirational Futures 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 (2023) 'Data protection in schools'

This policy operates in conjunction with the following school policies:

- Data Protection Policy
- Records Management Policy
- Cyber Response and Recovery 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 board is 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 CEO is 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 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.

Information will be included in the school's 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 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.

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

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 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 pupils' biometric data, the school will send pupils' parents/carers a Parental Notification and Consent Form for the use of Biometric Data. Written consent will be sought from at least one parent/carers of the pupil before the school collects or uses a pupil's biometric data.

The name and contact details of pupils' parents/carers will be taken from the school's admission register.

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

Parents/carers, and pupils, will be made aware that they can object to participation in the school's biometric systems or withdraw their consent at any time, and that if they do this, the school will provide them with an alternative method of accessing the relevant services.

Where a pupil or their parent/carer objects, 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.

Where staff members or other adults use the school's biometric systems, 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 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 school's biometric systems, in line with the Alternative arrangements section of this policy.

7. Alternative arrangements

Pupils, staff members and other relevant adults have the right to not take part in the school's biometric systems.

Where an individual objects to taking part in the school's 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 school meals, the pupil will be able to use a pin number 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.

8. Storage and data retention

Biometric data will be managed and retained in line with the school's Records Management Policy.

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

If an individual withdraws their consent for their or their child's biometric data to be processed, it will be erased from the school's 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 school.

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 school's Data and Cyber-security Breach Prevention and Management Plan.

10. Monitoring and review

The governing board will review this policy on an annual basis. The next scheduled review date for this policy is September 2024.

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

Notification of intention to process pupils' biometric information and consent form

Dear Parent/Carer,

I am writing to notify you of the school's wishes to use information about your child as part of an automated recognition system. The purpose of this system is to facilitate catering transactions to be made using pupils' fingerprints, instead of by using cash.

We believe this provides the school with a number of very significant benefits including:

- Reduction administration time and cost dealing with lost or forgotten cards/password/PINs.
- Reduction in the need for cash handling
- Reduction in queuing time.

Under the Protection of Freedoms Act 2012, we are required to notify parents/carers of a child, and obtain the written consent of at least one parent/carer before being able to use a child's biometric information for an automated system.

Consent given by one parent/carer will be overridden if another parent/carer objects in writing to the use of their child's biometric information. Similarly, if your child objects to the use of their biometric information, the school cannot collect or use the information for inclusion on the automated recognition system.

You can also object to the proposed processing of your child's biometric information at any time or withdraw any consent you have previously given. Please note that you must make any consent, withdrawal of consent or objection in writing.
Even if you have given your consent, your child can object or refuse at any time to their biometric information being collected and used – their objection does not need to be in writing. We would appreciate if you could discuss this with your child and explain to them that they can object if they want to.

If you do not wish for your child to use the Biometric System, or your child objects to such processing, they will be issued with a unique PIN number instead. If this is the case, you do not need to complete the form.

If you would like more information or the chance to discuss this further, please feel free to contact me.

Yours faithfully,

Mr A Dowsing
Trust Network Manager

CONSENT FORM FOR THE USE OF BIOMETRIC INFORMATION IN SCHOOL

Please complete this form if you consent to your child using biometric systems at School for use with the cashless catering system until he/she leaves the school.

I give consent to the school for biometrics of my child to be used by the School.

Name of pupil: .....

Form/Year .....

Name of parent/carer: .....

Signature of parent/carer: .....

Date: .....