



# PROTECTION POLICY

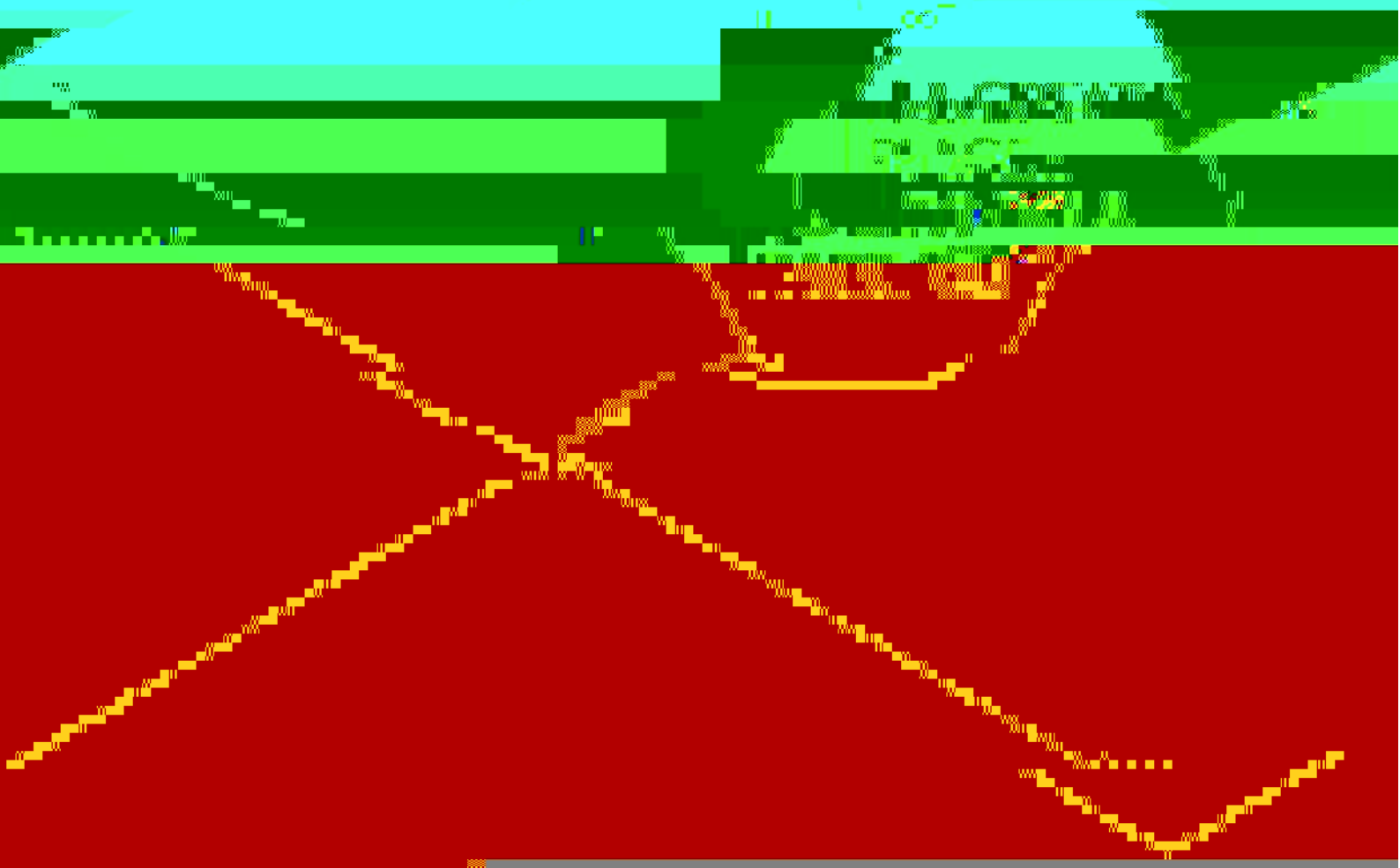
Policy Number: 86

Version Number: 07

Ratified by Trustees: 17th April 2024

17th April 2025

Link: Mr J Lowe



## STATEMENT OF INTENT - PROTECTION OF BIOMETRICS

The intent of protecting the personal data of all pupils at Horsted Primary includes the use of biometric data we collect and process. We collect and process biometric data in accordance with relevant legislation and guidance to ensure the data is protected. This includes the use of biometric data to ensure the school follows the correct procedures when collecting and processing biometric data.

### 1. LEGAL FRAMEWORK

- 1.1. This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:
  - 1.1.1. Protection of Freedoms Act 2012
  - 1.1.2.
  - 1.1.3. UK General Data Protection Regulation (UK GDPR)
  - 1.1.4.
- 1.2. This policy operates in conjunction with the following school policies:
  - 1.2.1. Data Protection Policy
  - 1.2.2. Records Management Policy

### 2. DEFINITIONS

- 2.1. Biometric data: Personal information about an individual's physical or behavioural characteristics that can be used to identify or verify the individual's identity, such as facial features, fingerprints, patterns, and hand measurements.
- 2.2. Behavioural characteristic: A characteristic of an individual that can be used to identify or verify the individual's identity. 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.
  - 2.3.1. Recording pupils' biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.
  - 2.3.2. Storing pupils' biometric information on a database.

2.3.3. ~~Where possible, the use of biometric data should be avoided, and where it is used, it should be used in a way that is consistent with the principles set out in the GDPR.~~

2.4. Special category data: Personal data which the GDPR says is more sensitive, and so needs more protection – ~~where biometric data is used for identification purposes, it is considered special category data.~~

### 3. ROLES AND RESPONSIBILITIES

3.1.

3.1.1. Reviewing this policy on an annual basis.

3.2. The Principal is responsible for:

3.2.1. ~~Ensuring the provisions in this policy are implemented consistently.~~

3.3. The data protection officer (DPO) is responsible for:

3.3.1. ~~Monitoring the school's compliance with data protection legislation in relation to the use of biometric data.~~

3.3.2. ~~Advising on when it is necessary to undertake a data protection impact assessment (DPIA) in relation to the school's biometric system(s).~~

3.3.3. ~~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

4.1. ~~The school processes all personal data, including biometric data, in accordance with the principles set out in the GDPR.~~

4.2. ~~The school captures biometric data in:~~

4.2.1. ~~Processed lawfully, fairly, and in a transparent manner~~

4.2.2. ~~Only collected for specified, explicit and legitimate purposes, and not further processed in a way that is incompatible with those purposes~~

4.2.3. ~~Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.~~

4.2.4. ~~to data and that appropriate measures are taken to ensure that the data is protected in a way that is consistent with the principles set out in the GDPR.~~

4.2.5.

## 6. NOTIFICATION AND CONSENT



- 6.1. ~~(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.~~
- 6.2. ~~When a pupil starts at the school, the school will obtain the parent's consent for the school to use the pupil's Biometric Data.~~
- 6.3. ~~Written consent will be sought from at least one parent of the pupil before the school collects or uses a pupil's biometric data.~~
- 6.4. ~~The school will not register any biometric data with the school's admissions register.~~
- 6.5. ~~If a pupil enrolls in a school through the school's admissions register, the Principal will consider the school's own policies on biometric data and the school's own policies on biometric data.~~
- 6.6. ~~The school does not need to notify a particular parent or seek their consent if it is satisfied that:~~
  - 6.6.1. ~~The parent is unable to provide their consent because of their mental capacity;~~
  - 6.6.2. ~~The parent lacks the mental capacity to object or consent;~~
  - 6.6.3. ~~The parent is unable to provide their consent because the parent has been separated from an abusive parent who must not be informed of the pupil's whereabouts;~~
  - 6.6.4. ~~It is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.~~
- 6.7. ~~Written 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.~~

  - 6.7.2. ~~and written consent will be obtained from at least one parent before the pupil's biometric data can be processed.~~



## 7. ALTERNATIVE ARRANGEMENTS

- 7.1. Where an individual objects to taking part in the school's biometric system(s) reasonable alternative arrangements will be made to allow the individual to access the relevant service using an alternative method.
- 7.2. Where an individual objects to taking part in the school's biometric system(s) reasonable alternative arrangements will be made to allow the individual to access the relevant service using an alternative method. For example, if a pupil's fingerprints do not scan, the school will have a backup system in place for the pupil to use, such as a PIN code or a password, to access the service. The school will also have a backup system in place for the pupil's parents to use, such as a PIN code or a password, to access the service.
- 7.3. 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).

## 8. DATA RETENTION

- 8.1. Biometric data will be managed and retained in line with the Trust's Records Management Policy.
- 8.2. 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.

## 9. BREACHES

- 9.1. There are appropriate and robust security measures in place to protect the biometric data held by the school.
- 9.2. Any breach to the school's biometric system(s) will be dealt with in accordance with the Data Protection Policy.

## 10. MONITORING AND REVIEW

- 10.1. The Board of Trustees will review this policy on an annual basis.
- 10.2. The next scheduled review date for this policy is 24<sup>th</sup> April 2024.
- 10.3. The school will ensure that this policy is kept up to date and reflects any changes in legislation or best practice.