

**Data Protection**

Protection of Biometric Information Policy

**At September 2020 no biometric information is stored or used**

*As a Christian school our vision is to promote ‘Life in All its Fullness.’ Our ethos is based on our 12 Christian values of hope, honesty, patience, joy, forgiveness, tolerance, thankfulness, respect, kindness, friendship, gentleness and love. It is within the vision and the ethos that this policy is written and will be implemented.*

Date Issued: September 2020

Review Date: July 2021 – in line with Data Protection Policy

Signed: …………………………………………………………………………………… Chair Pupil Support

**Contents**

[**Statement of intent** 3](#_Toc56507459)

[1. Legal framework 3](#_Toc56507460)

[2. Definitions 3](#_Toc56507461)

[3. Roles and responsibilities 4](#_Toc56507462)

[4. Data protection principles 4](#_Toc56507463)

[5. Data protection impact assessments (DPIAs) 5](#_Toc56507464)

[6. Notification and consent 5](#_Toc56507465)

[7. Alternative arrangements 6](#_Toc56507466)

[8. Data retention 7](#_Toc56507467)

[9. Breaches 7](#_Toc56507468)

[10. Monitoring and review 7](#_Toc56507469)

## **Statement of intent**

Holly Hill 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 follow when collecting and processing biometric data.

# Legal framework

* 1. This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:
* Protection of Freedoms Act 2012
* Data Protection Act 2018
* General Data Protection Regulation (GDPR)
* DfE (2018) ‘Protection of biometric information of children in schools and colleges’
	1. This policy operates in conjunction with the following school policies:
* Data Protection/GDPR Policy
* Records Management Policy
* E-Safety and Acceptable use

# Definitions

2.1 **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.

2.2 **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.

2.3 **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.

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.

# Roles and responsibilities

3.1 Holly Hill Governing body is responsible for reviewing this policy in line with the Data Protection policy.

3.2 The Head Teacher is responsible for ensuring the provisions in this policy are implemented consistently.

 3.3 The Data Protection Officer (DPO) is responsible for:

* Monitoring 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.

# Data protection principles

Holly Hill processes all personal data, including biometric data, in accordance with the key principles set out in the GDPR. The school 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. In line with the Records management policy.

# Data protection impact assessments (DPIAs)

Prior to processing biometric data or implementing a system that involves sharing or 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.

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.

# Notification and consent

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

Consent will be sought from at least one parent/carer of the pupil before the academy collects or uses a pupil’s biometric data.

6.1 The name and contact details of the pupil’s parents/carers will be taken from the schools SIMS database.

6.2 If a child is locked after, 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.

6.3 Notification sent to parents/carers 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/carer’s and the pupil’s right to refuse or withdraw their consent
	1. Parents/carers and pupils can object to participation in the 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.
	2. Where staff members or other adults use any biometric system(s), consent will be obtained from them before they use the system.
	3. 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

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

7.2 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/carers, where relevant).

# Data retention

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

# Breaches

9.1 There are appropriate and robust security measures in place to protect the biometric data held

9.2 Any breach to the academy’s biometric system(s) will be dealt with by the DPO.

# Monitoring and review

10.1 The Protection of Biometric information Policy will be reviewed in line with the Data protection policy.

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