



The Crypt School

Protection of Biometric Information Policy

Lead Persons: Gordon Taylor, IT Manager; Nicola Donlon, Compliance Officer
SLT Member Responsible: Senior Deputy Headteacher
Governing Body Committee: Pupil Education and Outcomes

The Crypt School is committed to protecting the personal data of all its pupils and staff, including 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 procedures the School follows when collecting and processing biometric data.

1. LEGAL FRAMEWORK

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
- The UK General Data Protection Regulation (UK GDPR)
- Department for Education (2022) '*Protection of biometric information of children in schools and colleges*'

This policy operates in conjunction with the School's Data Protection Policy.

2. 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.

3. ROLES AND RESPONSIBILITIES

The Headteacher is responsible for ensuring that the provisions in this policy are implemented.

The School's data protection officer (DPO) is responsible for:

- Monitoring the School/Academy'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/Academy's biometric system(s).
- Being the first point of contact for the Information Commissioner's Office.

4. DATA PROTECTION PRINCIPLES

The Data Protection Act 2018, UK GDPR and the Protection of Freedoms Act 2012 set out how students' and staff's data (including biometric data, which is a form of special category data) should be processed. 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.

5. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Prior to processing biometric data or implementing a system that involves processing biometric data, the School will seek the Data Protection Officer's advice on whether a DPIA should be carried out.

6. PROVIDING CONSENT/OBJECTING

Pupils under the age of 18

The specific obligations concerning consent for the processing of biometric information of children under the age of 18 are imposed by 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 for cashless catering payments), the School will comply with the requirements of the Protection of Freedoms Act 2012 and the associated Department for Education guidance, *Protection of Biometric Information of Children in Schools and Colleges* (updated July 2022):

- The School must obtain consent for the processing of biometric information of children under the age of 18;

- The School must notify each parent¹ of a pupil under the age of 18 if it wishes to take and use the child's biometric data as part of an automated biometric recognition system. This requirement does not apply if the parent cannot be found; their whereabouts or identity are not known; the welfare of the child requires that a particular parent/carers is not contacted; the parent lacks the mental capacity to object or to consent; or where it is otherwise not reasonably practicable for a particular parent to be contacted or their consent obtained. Where neither of the parents of a child can be notified, section 27 of the Protection of Freedoms Act 2012 sets out who should be notified and who can give consent.
- Written consent must be obtained from at least one parent of the pupil before the School collects or uses a pupil's biometric data.
- The School must not process the biometric data of a pupil under 18 years of age where:
 - The pupil (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
 - No parent has consented in writing to the processing; or
 - A parent has objected in writing to such processing, even if another parent has given consent.
- The School must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system. Alternative arrangements must ensure that pupils do not suffer any disadvantage or difficulty in accessing the relevant service, and should not place any additional burden on parents whose children are not participating in an automated biometric recognition system.

Notification sent to parents or others responsible for providing consent 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 the 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.

Staff and other adults (aged 18 or over)

The legal basis under the UK GDPR and Data Protection Act 2018 for processing the biometric data of adults will be that of consent, and the consent provisions of that legislation shall apply.

Where staff members or other adults use the School's biometric system(s), written consent will be obtained from them before they use the system. Notification provided before providing consent will include information regarding the following:

- Details about the type of biometric information to be taken.
- How the data will be used.
- The individual's right to refuse or withdraw their consent.
- The reasonable alternative arrangements in place for those who do not wish their biometric information to be processed for this purpose.

¹ This term includes any individual with parental responsibility for the child under the meaning set out by Part 1 of the Children Act 1989

Withholding or withdrawing consent

Parents, pupils and staff can object to participation in the School/Academy's biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted. If a pupil under the age of 18 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).

7. DATA RETENTION

When a pupil or member of staff leaves the School or ceases to use the biometric system, their biometric information will be securely erased within one month of that event, in accordance 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.

8. ENQUIRIES AND COMPLAINTS

Questions or concerns about the way the School is collecting or using biometric data may be raised in the first instance by contacting the Compliance Officer (foi@crypt.gloucs.sch.uk). Complaints made to the School will be handled using the School's Complaints Procedure (see school website).

Alternatively, you can contact the School's Data Protection Officer at: Gloucestershire County Council, School's Data Protection Team, Information Management Service, Shire Hall, Westgate Street, Gloucester GL1 2TG (email schoolsdpo@gloucestershire.gov.uk).

Should you wish to, you may make a complaint to the Information Commissioner's Office at <https://ico.org.uk/concerns/>; Tel: 0303 123 1113

Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Approved by Pupil Education and Outcomes Committee: June 2028

Review cycle: 2 years

Date of next review: June 2028