Protection of Biometric Information Policy

THE SPIRES COLLEGE

Contents

1 Policy Statement

The Spires College is committed to protecting the personal data of all its students 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 the individual are protected. This policy outlines the procedures the College follows when collecting and processing biometric data.

2 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
- General Data Protection Regulation (GDPR)
- DfE (2018) 'Protection of Biometric Information of Children in Schools and Colleges'

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 student/staff biometric data *e.g. taking measurements from a fingerprint via a fingerprint scanner*
- Storing student/staff biometric data information on a database
- Using student/staff biometric data as part of an electronic process *e.g. by comparing it with biometric information stored on a database to identify or recognise students*

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.

4 Roles and Responsibilities

The **Governing Body** is responsible for:

- Reviewing this policy annually

The **Business Manager** is responsible for:

- Ensuring the provisions in this policy are implemented consistently

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

- Monitoring the College'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 College's biometric system(s)
- Being the first point of contact for the ICO and for individuals whose data is processed by the College and connected third parties

5 Data Protection Principles

The College processes all personal data, including biometric data, in accordance with the data protection principles set out in legislation and in the College's Data Protection Policy.

The College ensures that biometric data is:

- Processed lawfully, fairly and in a transparent manner
- 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
- Kept in a form which permits identification of individuals 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 personal data.

6 Data Protection Impact Assessments (DPIAs)

Prior to processing biometric data or implementing a system that involves processing biometric data, a Data Protection Impact Assessment (DPIA) will be carried out.

The Data Protection Officer (DPO) will oversee and monitor the process of carrying out the DPIA.

The DPIA will:

- Describe the nature, scope, context and purpose 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 Information Commissioner's Office (ICO) before the processing of biometric data begins. The ICO will provide the College with a written response (within eight weeks or 14 weeks in complex

cases) advising whether the risks are acceptable, or whether the College needs to take further action. In some cases, the ICO may advise the College to not carry out the processing.

7 Consent

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 are imposed by Section 26 of the Protection of Freedoms Act 2012.

Where the College uses students and staff biometric data as part of an automated biometric recognition system *(e.g. using students' fingerprints to receive school dinners instead of paying with cash)* the College will comply with the requirements of the Protection of Freedoms Act 2012.

Written consent will be sought from at least one parent/carer of the student before the College collects of uses a student's biometric data. The name and contact details of the student's parents/carers will be taken from the College's admissions register. Where the name of only one parent/carer is included on the admissions register, the Principal will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent/carer.

The College does not need to notify a particular parent/carer or seek their consent if it is satisfied that:

- The parent/carer cannot be found *(e.g. their whereabouts or identity is unknown)*
- The parent/carer lacks the mental capacity to object or consent
- The welfare of the student requires that a particular parent/carer is not contacted *(e.g. where a student has been separated from an abusive parent/carer who must not be informed of the student's whereabouts)*
- It is otherwise not reasonable practicable for a particular parent/carer to be notified or for their consent to be obtained

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/carer's and the student's right to refuse or withdraw their consent
- The College's duty to provide reasonable alternative arrangements for those students whose information cannot be processed

The College will not process the biometric data of a student under 18 in the following circumstances:

- The student (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data
- No parent/carer has consented in writing to the processing
- A parent/carer has objected in writing to the processing, even if another parent/carer has given written consent

Parent/carers and students can object to participation in the College's biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the student that has already been captured will be deleted.

If a student objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the College will ensure that the student's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the student's parent(s).

Where staff members or other adults use the College'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 College'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 College's biometric system(s), in line with section 8 of this policy.

8 Alternative Arrangements

Where an individual objects to taking part in the College'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 a student's fingerprints to pay for school meals, the student will be able to use a pin code for the transaction instead.

Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service.

9 Data Retention

Biometric data will be managed and retained in line with in accordance with the **IRMS Information Management Toolkit for Schools.**

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

10 Policy Monitoring and Review

The Governing Body will review this policy annually.

11 Further Information and Guidance

This can be found via the following links

Department for Education's 'Protection of Biometric Information of Children in Schools – Advice for proprietors, governing bodies, head teachers, principals and school staff

ICO guidance on data protection for education establishments