STUDENT BIOMETRIC DATA POLICY

For

Stretford Grammar School

June 2023

Student Biometric Data Policy

Introduction

Biometric systems are used within Stretford Grammar School to make certain processes within school more efficient. When processing biometric data, we must ensure that we do so in accordance with the relevant legislation, not only to ensure compliance but to support the rights and freedoms of the students whose biometric data is processed by these systems. This policy outlines the school's approach to processing biometric data.

Legal Framework

When processing biometric data, the school comply with the following legislation:

- Data Protection Act (2018)
- UK General Data Protection Regulation (UK-GDPR)
- Protection of Freedoms Act (2012)

The following guidance has also been considered when collating this policy:

- Department for Education (DfE) 'Protection of Biometric Information of Children in Schools and Colleges' (2022)

This policy should be read in conjunction with the schools 'Data Protection Policy'.

Responsibilities

The Headteacher is responsible for ensuring that this policy is implemented effectively and that adequate resources are available to manage the processing of biometric data.

The Data Protection Officer (DPO) is responsible for:

- monitoring compliance with data protection legislation in respect of biometric data
- advising on data protection impact assessments for biometric processing
- being the first point of contact for individuals and the Information Commissioners Office (ICO).

All staff are responsible for complying with this policy when processing biometric data. Noncompliance with this policy may result in disciplinary action.

What is Biometric Data?

Biometric data is personal information about a person's physical or behavioural characteristics that can be used to identify them. Common examples of biometric data include the use fingerprint and facial recognition.

Biometric data is classed as 'special category' information under the UK-GDPR which means it is much more sensitive in nature and requires extra safeguarding to keep it secure and protected.

How we use Biometric Data?

The type of systems used within school to process biometric data are referred to as an 'automated biometric recognition systems'. This means these systems can automatically recognise a person, in this case our students via a measurement of their biometric data.

The school currently process student fingerprints using automated biometric recognition systems in order to manage the following processes more effectively:

- Recording and monitoring attendance.
- Managing access in and out of certain areas of the school. - Managing lunchtime meal provision and payments.

If a parent or carer consents to the processing of their childs biometric data for the purposes outlined above, a scanned measurement of the fingerprint will be taken and stored electronically within a database. This measurement is linked to a user profile for the student which automatically updates each time their fingerprint is scanned when partaking in the activities listed above.

Data Protection and Biometric Data

As biometric data can identify an individual, it is classed as personal data under data protection legislation. The school therefore must comply with the following key principles of the UK-GDPR and ensure that biometric data is:

- Processed lawfully, fairly and in a transparent manner.
- Only collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes.
- Adequate and limited to what is strictly necessary in relation to the specific purposes for which it was collected.
- Accurate and where necessary kept up to date and reasonable steps taken to ensure inaccurate or incomplete information is rectified.
- Kept no longer than necessary for the purposes for which it is was collected.
- Processed in a manner that ensures the appropriate security, integrity and confidentiality of the data is maintained by implementing appropriate technical and organisational control measures.

Processing biometric data lawfully, fairly and in a transparent manner

The processing of biometric data by the school and / or college for individuals under the age of 18 is governed by the 'Protection of Freedoms Act'. The act imposes a requirement for the school to inform parents/carer or carers of the processing of their childs biometric data along with obtaining their consent prior to any processing taking place.

As part of the consent process, the school provide parents/carer and students with clear information outlining the following details:

- The type of biometric data the school wishes to process.
- The intended use and purpose.
- That the processing is completely optional and that alternative provisions are available should the parent object to having their child's biometric data processed.
- Informing the parent that their child has a right to object and override parental consent.
- Instructions on how to withdraw their consent or change their preferences at any time if they wish to do so.

Parents/carer and carers are issued with a consent form detailing the information above along with clear options to consent or object to processing. Student biometric data will not be processed unless written consent has been obtained from at least one parent or carer (who has authority or parental responsibility for the child).

In situations where only one parent is listed on the schools' register, a reasonable attempt will be made to obtain details of the other parent to notify them (where feasible) of the schools wish to process their childs biometric data.

The school will not notify or seek consent from parents/carer in the following circumstances:

- The parent cannot be found or their identity / whereabouts are not known.
- The parent lacks mental capacity to object or consent.
- The welfare of the child requires that a particular parent is not contacted; when a child is looked after for instance.
- Where it is not reasonably practicable for a particular parent to be notified or consent to be obtained.

In situations where the school has been unable to notify or obtain consent from either parent for the reasons set out above, the Local Authority or organisation authorised to care for the child will be notified and consent sought from at least one carer prior to any processing of biometric data.

Student Right to Refuse

Under the Protection of Freedoms Act, students have a right to object to the processing of their own biometric data, this right overrides any consent provided by a parent or carer. The school inform students of their right to object prior to the processing of their biometric data and provide details of alternative arrangements.

If a student objects prior to any of their biometric data being processed, the school will refrain from any processing. In situations where biometric data has already been processed and a student changes their mind, no further processing will take place. Steps will be taken to ensure any biometric data stored is securely destroyed from applicable automated biometric recognition systems.

The school will inform the student and parent of the alternative options available to ensure access to the relevant services is maintained. The school understand that alternative provisions should not disadvantage students or place any additional burden on parents/carer. Alternative access to services are established prior to any biometric system being implemented.

Ensuring biometric data is only processed for specific, explicit and legitimate purposes.

The school only process biometric data to meet the purposes for which it was collected. Automated biometric recognition systems are carefully selected and designed to ensure biometric data is only used for specific purposes. Data sharing agreements are in place with third party system providers to ensure all parties are aware of their responsibilities and the schools' expectations.

If the school intends to process biometric data of its staff and students for a new purpose, a Data Protection Impact Assessment (DPIA) will be conducted and if approved, consent forms amended and re-issued to all parties whose data is processed.

The processing of biometric data should be adequate and strictly limited to what is necessary.

Prior to processing biometric data, an assessment will be made as part of the DPIA to ascertain what data is essential to meet the necessary purpose it is being collected for. Biometric data is currently limited to student fingerprints. Only a measurement of the fingerprint is taken; an images of the students fingerprint is not stored.

The school retain full control of the categories of data processed on automated biometric recognition systems.

Biometric data should be kept up to date and accurate.

Consent for the processing of biometric data is reviewed and updated on a routine basis if any change in preferences is received from the individual. The school retain an active log of consent that is accessible to relevant staff members to ensure biometric data is only processed where valid consent is in place.

Provisions are in place to ensure biometric data can be re-scanned and measured if an issue with the system occurs.

Biometric data is not kept for longer than necessary.

Biometric data is securely destroyed in the following situations:

- Consent to processing is withdrawn.
- A student objects to processing
- Processing is no longer required by the school.

As a rule of thumb, the school perform a bulk deletion of student biometric data from the relevant systems once students leave in Year 11 and Sixth Form. Ad-hoc deletions will be applied in situations where consent is withdrawn, or an objection request is made.

Activity logs created via biometric data processing such as attendance and lunchtime records will be retained for longer; the school has legal obligations to keep such records for the set periods outlined in our 'Records Management & Retention Policy'.

Agreements are in place with third party providers of automated biometric recognition systems to ensure actions can be taken to securely destroy biometric data upon the school's request.

Biometric data should be processed in a manner that ensures appropriate security, integrity and confidentiality.

Prior to implementing biometric data processing, the school conduct a DPIA to assess the level of risk to the privacy of individuals involved. As part of this process, a compliance check is conducted on third party providers of automated biometric recognition systems to ensure that they:

a. Meet the high levels of data protection compliance expected by the school.
b. Have adequate control measures and technical security in place to ensure any biometric and other personal data processed by the school is as secure as possible.

The school do not process biometric data via a third party without a strict agreement in place outlining the schools' expectations. Nor do the school process biometric data unless it is satisfied that any risks identified in the DPIA have been alleviated.

Staff access to biometric data systems is only permitted if it is necessary to perform their roles; only a select few staff members have full management control of systems to administer use and access. Staff will be permitted certain levels of access to systems dependent upon what they need to perform their role.

Biometric data is stored on secure encrypted servers; staff and students have a dedicated user account accessible via a password and / or a fingerprint scan for students.

DPIA's and the risks associated with biometric data processing are assessed on a routine basis. If the school is notified of a security concern, processing will be restricted until an adequate solution has been implemented.

Supporting the Rights of Data Subjects

The school have implemented the use of biometric data into the relevant 'Privacy Notices' to ensure it is clear how and why the biometric data of staff and students is processed. Privacy Notices are accessible to all individuals via the school office and website.

In addition to this policy, a FAQ sheet is available for parents/carer at Appendix A to outline answers to some of the key questions they may have regarding the biometric processing of their childs data. Appendix B includes the schools latest notification to parents/carer which is published on our website.

All parents/carer and carers are provided with a consent form and information that clearly notifies them of the intended use of their childs biometric data along with their right to withdraw consent and information on their childs right to object.

Provisions are in place to ensure any processing of biometric data is halted without undue delay if consent is withdrawn or an objection to processing is received. The school will action the secure deletion of biometric data stored on the system.

Automated biometric recognition systems utilised by the school are designed in a manner that support the extraction of user data should a request be made to access personal information. Similarly, information is kept up to date each time activity takes place on the user's account; automatic syncing with the school's key information management system ensures that any accompanying personal data that is amended also updates automatically in the biometric system.

Complaints

The school ask that any concerns regarding this policy or the processing of biometric data is raised with the school in the first instance to give us the opportunity to resolve your complaint.

Individuals also have the right to complain to the Information Commissioners Office (ICO) using the following link: https://www.ico.org.uk

Appendix A – Biometric Data – FAQs

What information should schools provide to parents/carer/students to help them decide whether to object or for parents/carer to give their consent?

Any objection or consent by a parent must be an informed decision – as should any objection on the part of a child. School will take steps to ensure parents/carer receive full information about the processing of their child's biometric data including a description of the kind of system we use, the nature of the data we process, the purpose of the processing and how the data will be obtained and used. Children will be provided with information in a manner that is appropriate to their age and understanding.

What if one parent disagrees with the other?

The school is required to notify each parent of a child whose biometric information we wish to collect / use. If one parent objects in writing, then the school will not be permitted to take or use that child's biometric data.

How will the child's right to object work in practice – must they do so in writing?

A child is not required to object in writing. An older child may be more able to say that they object to the processing of their biometric data. A younger child may show reluctance to take part in the physical process of giving the data in other ways. In either case the school will not be permitted to collect or process the data.

Are schools required to ask/tell parents/carer before introducing an automated biometric recognition system?

Schools are not required by law to consult parents/carer before installing an automated biometric recognition system. However, they are required to notify parents/carer and secure consent from at least one parent before biometric data is obtained or used for the purposes of such a system. It is up to schools to consider whether it is appropriate to consult parents/carer and students in advance of introducing such a system.

Do schools need to renew consent every year?

No. The original written consent is valid until such time as it is withdrawn. However, it can be overridden, at any time if another parent or the child objects to the processing (subject to the parent's objection being in writing). When the student leaves the school, their biometric data should be securely removed from the school's biometric recognition system.

Do schools need to notify and obtain consent when the school introduces an additional, different type of automated biometric recognition system?

Yes, consent must be informed consent. If, for example, a school has obtained consent for a fingerprint/fingertip system for catering services and then later introduces a system for accessing library services using thumbprints or retina scanning, then the school will meet the notification and consent requirements for the new system in writing.

Can consent be withdrawn by a parent?
Parents/carer will be able to withdraw their consent, in writing, at any time. In addition, either parent will be able to object to the processing at any time, but they must do so in writing to the Data Manager in school.

When and how can a child object?

A child can object to the processing of their biometric data or refuse to take part at any stage – i.e. before the processing takes place or at any point after his or her biometric data has been obtained and is being used as part of a biometric recognition system. If a student objects, the school must not start to process his or her biometric data or, if they are already doing this, must stop. The child does not have to object in writing.

Will consent given on entry to primary or secondary school be valid until the child leaves that school?

Yes. Consent will be valid until the child leaves the school – subject to any subsequent objection to the processing of the biometric data by the child or a written objection from a parent. If any such objection is made, the biometric data should not be processed and the school will, in accordance with the GDPR, remove it from the school's system by secure deletion.

Can the school notify parents/carer and accept consent via email?

Yes – as long as the school is satisfied that the email contact details are accurate, and the consent received is genuine.

Is parental notification and consent required under the Protection of Freedoms Act 2012 for the use of photographs and CCTV in schools?

Not unless the use of photographs and CCTV is for the purposes of an automated biometric recognition system. The school comply with the requirements of the UK General Data Protection Regulation (UK-GDPR) and Data Protection Act (DPA) when using CCTV for general security purposes or when using photographs of students for identification or promotional activities relating to the school such as on displays and the school website.

Depending on the activity concerned, consent may be required under the UK-GDPR before personal data is processed. The Government believes that the GDPR requirements are sufficient to regulate the use of CCTV and photographs for purposes other than automated biometric recognition systems. Photo ID card systems, where a student's photo is scanned automatically to provide them with services, would come within the obligations on schools and colleges under sections 26 to 28 of the Protection of Freedoms Act 2012, as such systems fall within the definition in that Act of automated biometric recognition systems.

Is parental notification or consent required if a student uses or accesses standard commercial sites or software which use face recognition technology?

The provisions in the Protection of Freedoms Act 2012 only cover processing by or on behalf of a school or college. If a school or college wishes to use such software for school work or any school business, then the requirement to notify parents/carer and to obtain written consent will apply. However, if a student is using this software for their own personal purposes, then the provisions do not apply, even if the software is accessed using school or college equipment.

Appendix B – Website Notification for Parents/carer

Stretford Grammar School wishes to use information about your child as part of an automated (i.e., electronically operated) recognition system.

This is for the purposes of cashless catering and the library management system. The information from your child that we wish to use is referred to as 'biometric information'. Under the Protection of Freedoms Act 2012 (sections 26 to 28), we are required to notify each parent of a child and obtain the written consent of at least one parent before being able to use a child's biometric information for an automated system.

Biometric information and how it will be used?

Biometric information is information about a person's physical or behavioural characteristics that can be used to identify them, for example, information from their finger images.

The school would like to take and use information from your child's finger image and use this information for the purpose of providing your child with access to our cashless catering system and the library management system.

The information will be used as part of an automated biometric recognition system. The system takes measurements of your child's finger image and converts these measurements into a template to be stored on the system. An image of your child's finger is not stored. The template (i.e. measurements taken from your child's finger image) is what is used to permit your child to access the cashless catering system and the library management system.

You should note that the law places specific requirements on schools when using personal information, such as biometric information, about students for the purposes of an automated biometric recognition system.