PROTECTION OF BIOMETRIC DATA POLICY (STUDENT & STAFF)

MIDDLEWICH HIGH SCHOOL

Last Reviewed September 2022

Amended: September 2022

Approved: FGB 27/09/2022

Next review date: September 2023

Document Control Information	
Document ID	**MHSADMIN&DATA006**
Document title	**MHS Protection of biometric data (Students & Staff) Policy**
Version	**1.2**
Status	**APPROVED**
Author	**Debbie Carter**
Publication date	**25/06/2018**
Next review date	**September 2023**

Version History			
Version	**Date**	**Detail**	**Author**
1.0	**13/07/2020**	**Initial**	**Rebecca Dale (RDA)**
1.1	**09/03/2021**	**Reviewed & Updated**	**Rebecca Dale (RDA)**
1.2	**23/09/2022**	**Reviewed & Updated**	**Laura Platt (LPL)**

Approvals	
Approver	**Date**
Governing Body	25/06/2018
FGB	22/03/2021
FGB	27/09/2022

Protection of Biometric Data (Students & Staff) Policy

Contents

1. Legal framework

1.1. This policy has due regard to legislation, including, but not limited to the following:

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

1.2. This policy will also have regard to the following guidance:

- DfE (2018) 'Protection of biometric information of children in schools and colleges'

1.3. This policy will be implemented in conjunction with the following other school policies:

- Data Protection Policy
- Records Management Policy

2. Definitions

For the purpose of this policy:

2.1. Personal data refers to information that relates to an identified or identifiable, living individual (Data Subject), including an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.2. Sensitive personal data is defined in the GDPR as 'special categories of personal data', which includes the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

2.3 Biometric data is defined as personal data relating to the physical, physiological or behavioural characteristics of a person, confirming the unique identification of that person, such as facial images or fingerprints. In our case it is used as the cashless payment system in the canteen where students and staff use their fingerprints to pay for their lunch.

2.4 Automated biometric recognition system is 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.

2.5 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 students/staff biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.
- Storing students/staff biometric information on a database.
- Using students/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.

3. Principles and accountability

3.1 Biometric data will only be processed in line with the requirements of all appropriate legislation.

3.2 Biometric data will only be processed where that processing is identified as necessary.

3.3 The school will implement appropriate technical and organisational measures to demonstrate that biometric data is processed in line with the principles set out in the GDPR.

3.4 The school will ensure the rights and freedoms of individuals are not adversely affected by the processing of any biometric data and that all appropriate rights as laid down by the GDPR are enforced.
3.5 The school will provide comprehensive, clear and transparent privacy notices detailing the use of biometric data.
3.6 The school will implement measures that meet the principles of data protection, continuously creating and improving security features.
3.7 The school will produce Data protection Impact Assessments where the processing of personal data is likely to result in a high risk to the rights of the individual, where a major project requires the processing of personal data or before the introduction of new technology or a significant change to the way processing is performed.
3.8 Any processing of biometric data will be referred to the Data Protection Officer for assessment to ensure the school fully complies with its data protection responsibilities.

4. Data protection Lead (DPO)

4.1. The Trust is required to appoint a DPO in order to:

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws in relation to the use of biometric data.
- Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members in relation to the processing of biometric data.

4.2 The role of DPO will be carried out the CFO of The Sir John Brunner Foundation
4.3 The Trust will make freely available the contact details for their appointed DPO:
Kathryn McBurnie
Chief Financial Officer
Northwich, Cheshire. CW9 8AF
McBurnie_K.sjbf@sjd.ac.uk
01606810028

4.4 The school has appointed a Data Protection Lead, Mrs Laura Platt, responsible for day-to-day compliance with this policy. She can be contacted at: -

Middlewich High School,
King Edward Street,
Middlewich,
Cheshire
CW10 9BU
01606 537670
lplatt@mhs.school

5. Privacy by design and Data Protection Impact Assessments

5.1 The school will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into biometric processing activities.
5.2 Data Protection Impact Assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.
5.3 Prior to processing biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out.
5.4 DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur.

5.5 A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.
5.6 A DPIA may be used for more than one project, where necessary and where the aims and conditions of the project are the same.
5.7 The school will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

5.8 Where a DPIA indicates high risk data processing where an identified risk cannot be mitigated, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

6. Consent for the use of Biometric Data

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.
6.1 Where the school uses student and/or 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 school will comply with the requirements of the Protection of Freedoms Act 2012.
6.2 Both parents/individuals or agencies with identified parental responsibility will be informed of the plan to process biometric data.
6.3 Written consent will be sought from at least one parent of the student before the school collects or uses a student's biometric data. (See Appendix 1)
6.4 The name and contact details of the student's parents will be taken from the school's admission register which the school will ensure is up-to-date.
6.5 Where the name of only one parent is included on the admissions register, the Head will ensure all reasonable steps are taken to ascertain the details of the other parent.
6.6 The school does not need to notify a particular parent or seek their consent if it is satisfied that:

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

6.7.1 Where neither parent of a student can be notified for any of the reasons set out in 7.6, consent will be sought from the following individuals or agencies as appropriate:

- If a student 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.
- If the above does not apply, then notification will be sent to all those caring for the student and written consent will be obtained from at least one carer before the student's biometric data can be processed.

6.8 Notification sent to parents 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 and the student's right to refuse or withdraw their consent
- The school duty to provide reasonable alternative arrangements for those students whose information cannot be processed

6.9 The school will not process the biometric data of a student under the age of 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 or carer has consented in writing to the processing
- A parent has objected in writing to such processing, even if another parent has given written consent

6.10 Parents and students can object to participation in the school 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.

6.11 If a student 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 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).

6.12 Where staff members or other adults use the school`s biometric system(s), consent will be obtained from them before they use the system.

6.13 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.

6.14 Alternative arrangements will be provided to any individual that does not consent to take part in the school's biometric system(s).

7. Alternative Arrangements

7.11 Parents, students, staff members and other relevant adults have the right to not take part in the school's biometric system(s).

7.12 Where an individual objection to taking part in the school'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 student's fingerprints to pay for school meals, they will be provided with a pin number.

7.13 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 student's parents, where relevant).

8. Data retention

8.1. Data will not be kept for longer than is necessary in line with the schools Record Management/Retention Policy.

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

8.3 When a student or member of staff leaves the school or ceases to use the biometric system, their biometric

Appendix - Template Notification and Consent Form

NOTIFICATION OF INTENTION TO PROCESS STUDENTS' BIOMETRIC INFORMATION

Dear Parent/Carer

Middlewich High School have a cashless catering system that was implemented in November 2013. The system has allowed us to continue with the development of the school meal service and provide a more efficient, faster and ultimately better quality of service. This system incorporates the latest technology and eliminates the need for students to carry cash throughout the day, thus reducing the risk of bullying.

Middlewich High School wishes to use information about your child as part of an automated (i.e. electronically-operated) recognition 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 fingerprint. The school would like to take and use information from your child's fingerprint and use this information for the purpose of providing your child with food and drinks purchased from the school canteen.

The information will be used as part of an automated biometric recognition system. This system will take measurements of your child's fingerprint and convert these measurements into a template to be stored on the system. An image of your child's fingerprint is not stored. The template (i.e. measurements taking from your child's fingerprint) is what will be used to permit your child to access services.

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.

For example:

a) The school cannot use the information for any purpose other than those for which it was originally obtained and made known to the parent(s) (i.e. as stated above);

b) The school must ensure that the information is stored securely;

c) The school must tell you what it intends to do with the information;

d) Unless the law allows it, the school cannot disclose personal information to another person/body – you should note that the only person/body that the school wishes to share the information with is Chartwells. This is necessary in order to [say why it needs to be disclosed to the third party].

As part of our assessment into the suitability for employing a biometric recognition system we have conducted a Data Protection Impact Assessment and have consulted with the School's Data Protection Officer.

The school is also happy to answer any questions you or your child may have and any concerns can be referred to the school Data Protection Lead at school ataylor@mhs.school.

Frequently Asked Questions

21.9.1 What information should schools provide to parents/students to help them decide whether to object or for parents 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. Schools should take steps to ensure parents receive full information about the processing of their child's biometric data including a description of the kind of system they plan to use, the nature of the data they process, the purpose of the processing and how the data will be obtained and used. Children should be provided with information in a manner that is appropriate to their age and understanding.

21.9.2 What if one parent disagrees with the other?
The schools will be required to notify each parent of a child whose biometric information they wish to collect/use. If one parent objects in writing, then the school or college will not be permitted to take or use that child's biometric data.

21.9.3 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 or college will not be permitted to collect or process the data.

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

Schools are not required by law to consult parents before installing an automated biometric recognition system. However, they are required to notify parents 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 and students in advance of introducing such a system.

21.9.5 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.

21.9.6 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 iris or retina scanning, then schools will have to meet the notification and consent requirements for the new system.

21.9.7 Can consent be withdrawn by a parent?
Parents 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.

21.9.8 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 or college 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.

21.9.9 Will consent given on entry to 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 must, in accordance with the GDPR, remove it from the school's system by secure deletion.

21.9.10 Can the school notify parents 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.

21.9.11 Will parents be asked for retrospective consent?

No. Any processing that took place prior to the provisions in the Protection of Freedoms Act coming into force will not be affected. Any school wishing to continue to process biometric data must have already sent the necessary notifications to each parent of a child and obtained the written consent from at least one of them before continuing to use their child's biometric data.

21.9.11 Does the legislation cover other technologies such as a palm and iris scanning?

Yes. The legislation covers all systems that record or use physical or behavioural characteristics for the purpose of identification. This includes systems that use palm, iris or face recognition, as well as fingerprints.

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

No – not unless the use of photographs and CCTV is for the purposes of an automated biometric recognition system. However, schools must continue to comply with the requirements in the GDPR 2018 when using CCTV for general security purposes or when using photographs of students as part of a manual ID system or an automated system that uses barcodes to provide services to students. Depending on the activity concerned, consent may be required under the 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.

Please refer to the CCTV Policy for more information.

21.9.13 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 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 equipment

22. Data retention

22.1 Data will not be kept for longer than is necessary in line with the schools Record Management Policy.

22.2 Unrequired data will be deleted as soon as practicable.

22.3 Some educational records relating to former students or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

22.4 Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.