UK GDPR - PROTECTION OF BIOMETRIC INFORMATION POLICY

Non Sibi Sed Aliis

Your word is a lamp to my feet and a light to my path.
Psalm 119, vs 105

"Nothing is covered up that will not be revealed, or hidden that will not be known. Therefore whatever you have said in the dark shall be heard in the light, and what you have whispered in private rooms shall be proclaimed on the housetops." **Luke 12: 2-3**

This policy document and the content contained therein remains the responsibility of the Headteacher and Governing Body of the school. No amendments can be made without their express instructions and they remain the final arbiters in any matters relating to it.

Review Date: Summer Term 2023

Next Review Date: Summer Term 2024

Reviewed By: Ms K Kidd

APPROVED BY THE GOVERNING BODY - Summer Term 2023

This policy has been created in line with the DfE's 'Protection of biometric information of children in schools and colleges' guidance, alongside other relevant legislation. This guidance was last updated in March 2018, prior to the implementation of the GDPR and Data Protection Act 2018. We contacted the DfE, who confirmed they are updating the guidance to account for the GDPR – we will update this policy accordingly once the DfE's updated guidance has been published.

Contents:

Statement of intent

Balshaws Church of England High School 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 follows when collecting and processing biometric data.

Signed by:

Headteacher Date: 12th July 2023

Chair of governors Date: 12th July 2023

1. Legal framework

1.1. 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'

1.2. This policy operates in conjunction with the following school policies:

- Data Protection Policy
- Records Management Policy
- Data and E-Security Breach Prevention and Management Plan

2. 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.

3. Roles and responsibilities

3.1. The governing body is responsible for:

- Reviewing this policy on an annual basis.

3.2. The Headteacher is responsible for:

- Ensuring the provisions in this policy are implemented consistently.

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

- Monitoring the school'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'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.

4. Data protection principles

4.1. The school processes all personal data, including biometric data, in accordance with the key principles set out in the GDPR.

4.2. 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.

4.3. As the data controller, the school is responsible for being able to demonstrate its compliance with the provisions outlined in 4.2.

5. Data protection impact assessments (DPIAs)

5.1. Prior to processing biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out.

5.2. The DPO will oversee and monitor the process of carrying out the DPIA.

5.3. 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.

5.4. When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered.

5.5. If a high risk is identified that cannot be mitigated, the DPO will consult the ICO before the processing of the biometric data begins.

5.6. 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.

5.7. The school will adhere to any advice from the ICO.

6. 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.

6.1. Where the school uses pupils' biometric data as part of an automated biometric recognition system (e.g. using pupils' 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. Prior to any biometric recognition system being put in place or processing a pupil's biometric data, the school will send the pupil's parents a Parental Notification and Consent Form for the use of Biometric Data.

6.3. Written consent will be sought from at least one parent of the pupil before the school collects or uses a pupil's biometric data.

6.4. The name and contact details of the pupil's parents will be taken from the school's admission register.

6.5. Where the name of only one parent is included on the admissions register, the Headteacher will consider whether any reasonable steps can or should be 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 pupil requires that a particular parent is not contacted, e.g. where a pupil has been separated from an abusive parent who must not be informed of the pupil's whereabouts.
- It is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.

6.7. Where neither parent of a pupil can be notified for any of the reasons set out in 6.6, consent will be sought from the following individuals or agencies as appropriate:

- If a pupil 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 pupil and written consent will be obtained from at least one carer before the pupil'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 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

6.9. The school will not process the biometric data of a pupil under the age of 18 in the following circumstances:

- The pupil (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 pupils can object to participation in the school's 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.

6.11. If a pupil 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).

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), in line with section 7 of this policy.

7. Alternative arrangements

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

7.2. Where an individual objects 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 pupil's fingerprints to pay for school meals, the pupil will be able to use a pin number for the transaction instead.

7.3. 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, where relevant).

8. Data retention

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

8.2. 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.

9. Breaches

9.1. There are appropriate and robust security measures in place to protect the biometric data held by the school. These measures are detailed in the school's Data and E-Security Breach Prevention and Management Plan.

9.2. Any breach to the school's biometric system(s) will be dealt with in accordance with the Data and E-Security Breach Prevention and Management Plan.

10.Monitoring and review

10.1. The governing board will review this policy on an annual basis.

10.2. The next scheduled review date for this policy is **July 2024**.

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

Balshaw's
Church Of England High School

Date

Dear Parent/Carer

We are pleased to tell you that Balshaw's CE High School operates a cashless catering system. The system is provided by LiveReigster and provides us with a more efficient, faster and better quality of service in the school canteen. This system incorporates the latest biometric technology that will recognise the thumb of your child at the revaluation pay points and at the tills.

In preparation for your child joining us, we are asking for your consent to use your child's biometric data. We will require the consent of at least one parent in order that the biometric information of your child can be processed. Please be assured that this information remains within the school and that the biometric information taken is an algorithm and not the actual finger print.

In line with data protection legislation we do need positive consent from you to use biometrics and therefore require you to complete the online consent form included in the new starter information/SIMS Parent App. If you choose not to have your child registered on the Biometric System then they will be issued with a 4 digit PIN code. Please note that PIN codes do not have the same level of security and it will be your child's responsibility to remember the code and keep it secure at all times.

The attached information should answer any questions you may have, however, if you do have any queries, please contact the school office and we will do our best to answer them.

Could you please complete the online consent form via the new starter pack as soon as possible to allow us to make arrangements for your child to access catering.

Yours sincerely

K E Kidd

Ms K Kidd
Business Manager

FREQUENTLY ASKED QUESTIONS - BIOMETRICS

Q. **What is a cashless system?**

A. A Cashless Catering System is a solution which is purpose designed to meet the ever-evolving needs and demands of the catering provision, required by today's schools and academies. The Trust-e Cashless Solution allows schools to be better able to provide their students with a faster, more efficient and more appealing meal service.

Q. **What is 'biometric?'**

A. Biometric is simply a method of identifying an individual person. The Trust-e Cashless System uses an algorithm-based scan, which reads between 50 and 130 points on the finger/thumb. It is not a fingerprint in any way, shape or form and is of use only in the Cashless System.

Q. **How does a biometric system work?**

A. The information of a student, who has been biometrically registered, is stored on a secure biometric controller within the school, which only our provider, LiveRegister, can access with permission from the school. Once an account is credited, the student places their finger/thumb on the EPOS Terminal Biometric Reader, which looks up their account and allows them to purchase items using only this method of identification.

Q. **How does my child register on the biometric system?**

A. Your child will be required to place their thumb on the Biometric Reader twice to obtain a matching template, which only takes a few seconds. If you have chosen to opt-out of this procedure, your child will be presented with a 4 digit PIN code.

Q. **What methods of payment can be used to credit an account?**

A. Any amount can be credited to an account by way of any of the following methods. Once an account has been credited, the monies cannot be withdrawn and must be spent on the school meal/break services.

Cash at the Revaluation Units

Revaluation units will be sited at different locations within the school. These can be used to top up accounts by the student placing their registered thumb on the Biometric Reader or by entering their 4 digit PIN Code followed by inserting the accepted tender: £20, £10, £5 notes or £2, £1, 50p, 20p, 10p or 5p coins. Please note that copper coins are not accepted.

Online Payments

We have introduced online payments in partnership with the Cashless Catering Solution. You will receive further information and an invitation to register for ParentPay.

WHAT IS A BIOMETRIC ALGORITHM?

The individual templates are encrypted using a 256 bit AES key that is built into the scanner's hardware. Also the persisted file is encrypted using a different 256 bit AES key built into the matching algorithm supplied by Secugen and generated by a unique license purchased for each site. This is more secure than the ANSII and ISO standards that government department's use as the Secugen Template is encrypted and the ANSII and ISO standards are not. The template data is useless and cannot be interpreted back into a usable fingerprint image. If this was not the case then there would be no world standards and performance measures for such technologies. The data is stored in an array in the RAM of the Biometric Controller and is also permanently stored on the hard drive of the Bio Controller to be restored in the event of a reboot.

Below is an example of a template code for an individual finger.
0X417741414142514141414445415141414151415341414D415A414141414141417477454141 4C714777346C5869656D6C574945494A764A6B42466D6837616C4E764D704F517874517A706A4A395A31784935686C4177395366726E777645576357386C4573314B426F474431666941706755597 04C763168423642682A7043

The solution is secure because the matching can only be done by the individual's consent as the finger has to be presented to the device for matching. We do not hold images of fingerprints in our system.

The technology provided for this method of identification meets with BECTA guidelines and also allows students the option to opt out of the scheme and use a PIN number instead.

Also under the data protection act the school or caterer (the originator of the data) cannot allow access to this data by anyone for any other means than for the purpose the data was collected and that is to identify an individual within the solution we supply. Any biometric data that belongs to an individual that leaves the school is purged which also is in line with the BECTA guidelines.