Parklands High School

An Academy

Protection of Biometric Information Policy

Parklands High School

Last Reviewed; December 2021

Next Review; December 2022

Version 202122.ad.v1

Contents:

Statement of intent

Parklands 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.

1. Legal framework

This policy has due regard to all relevant legislation and statutory 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)
- DfE (2018) 'Protection of biometric information of children in schools and colleges'

This policy operates in conjunction with the following school policies:

- Data Protection Policy
- Records Management 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. All biometric data is personal data.

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 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.

Special category data: Personal data which the UK GDPR says is more sensitive, and so needs more protection. Where biometric data is used for identification purposes, it is considered special category data, e.g. keystroke analysis.

3. Roles and responsibilities

The governing board is responsible for reviewing this policy on an annual basis.

The headteacher is responsible for ensuring the provisions in this policy are implemented consistently.

The 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

The school processes all personal data, including biometric data, in accordance with the key principles set out in the UK GDPR. 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. Notification and consent

Please note: 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 UK GDPR. Instead, the consent requirements for biometric information are imposed by section 26 of 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 to receive school dinners instead of paying with cash), the school will comply with the requirements of the Protection of Freedoms Act 2012.

Prior to any biometric recognition system being put in place or processing pupils' biometric data, the school will send pupils' parents a Parental Consent Form for the use of Biometric Data. Written consent will be sought from at least one parent of the pupil before the school collects or uses a pupil's biometric data. The name and contact details of pupils' parents will be taken from the school's admission register.

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.

Where neither parent of a pupil can be notified for any of the reasons set out above, 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.

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

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

Parents and pupils will be made aware that they can object to participation in the school's biometric system(s) or withdraw their consent at any time, and that if they do this, the school will provide them with an alternative method of accessing the relevant services.

Where a pupil or their parents object, any biometric data relating to the pupil that has already been captured will be deleted. 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).

Where staff members or other adults use the school'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 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.

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 6 of this policy.

6. Alternative arrangements

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

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 personal pin number for the transaction instead.

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).

7. Data retention

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

There are appropriate and robust security measures in place to protect the biometric data held by the school. 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.

9. Monitoring and review

The governing board will review this policy on an annual basis. The next scheduled review date for this policy is December 2022.

PARKLANDS HIGH SCHOOL
LEARN | RESPECT | ASPIRE | ACHIEVE

Parklands High School I Southport Road I Chorley I Lancashire I PR7 1LL
Tel: 01257 264596 I Fax: 01257 261215 I Email: admin@parklandsacademy.co.uk
www.parklandsacademy.co.uk

Dear Parent/Carer

BioStore

Biometric System – Cashless Catering

Parklands High School uses a cashless catering system which allows the use of a pupils' fingerprint to make purchases from the canteen.

We believe this provides the school with a number of very significant benefits including:

- Reduction in administration time and cost dealing with lost or forgotten cards/passwords/PINs
- Reduction in opportunities for bullying as there is nothing that can be stolen for use by another student
- Reduction in the need for cash handling
- Reduction in queuing time

In order to comply with the provisions of the Protection of Freedoms Act 2012 we need written permission from a parent/carer.

If you do not wish for your child to use the Biometric System, they can be issued with a unique PIN number instead. If this is the case, you do not need to complete the form.

If you would like more information or the chance to discuss this further, please feel free to contact me.

Yours faithfully,

Mr A Dowsing
Network Manager

PARKLANDS HIGH SCHOOL
LEARN | RESPECT | ASPIRE | ACHIEVE

Parklands High School I Southport Road I Chorley I Lancashire I PR7 1LL
Tel: 01257 264596 I Fax: 01257 261215 I Email: admin@parklandsacademy.co.uk
www.parklandsacademy.co.uk

IMPORTANT NOTES FOR PARENTS

Background to the use of biometrics in school

For the sake of clarity, biometric data is information about someone's physical or behavioural characteristics that can be used to identify them. There are many possible biometrics, including for example, a digital photograph, fingerprint, or hand shapes. As part of our identity management systems, we currently record a biometric measurement taken from a finger, but not a fingerprint image. The information is stored in a highly secure database and is only used by the school to confirm who is using a range of services. In future we may use other biometric services where appropriate.

Our chosen solution allows us to use a secure database holding biometric data for use with the cashless catering system in our canteen. This means we store the least amount of data possible. This reduces the risk of loss of data.

The data that is held cannot be used by any other agency for any other purpose. The school will store the biometric information collected securely, in compliance with General Data Protection Regulation (GDPR). The school will not share this information with anyone else and will not unlawfully disclose it to any other person.

Current Legislation – The Protection of Freedoms Act 2012

This legislation requires schools to:

- Inform parents about the use of the biometric systems in the school and explain what applications use biometrics.
- Receive written permission from one parent/carer if the school is to process biometrics for their child.
- Allow children to choose an alternative way of being identified if they wish.

Should you agree to your child using the biometric system, is it important that you return the signed consent form. Please note that when he/she leaves the school, or if for any reason you wish to withdraw consent, their biometric data will be permanently deleted.

PARKLANDS HIGH SCHOOL
LEARN | RESPECT | ASPIRE | ACHIEVE

Parklands High School I Southport Road I Chorley I Lancashire I PR7 1LL
Tel: 01257 264596 I Fax: 01257 261215 I Email: admin@parklandsacademy.co.uk
www.parklandsacademy.co.uk

CONSENT FORM FOR THE USE OF BIOMETRIC INFORMATION IN SCHOOL

Please complete this form if you consent to your child using biometric systems at Parklands High School for use with the cashless catering system until he/she leaves the school.

I give consent to the school for biometrics of my child to be used by Parklands High School.

Name of pupil: .....

Form: .....

Name of parent/carer: .....

Signature of parent/carer: .....

Date: .....