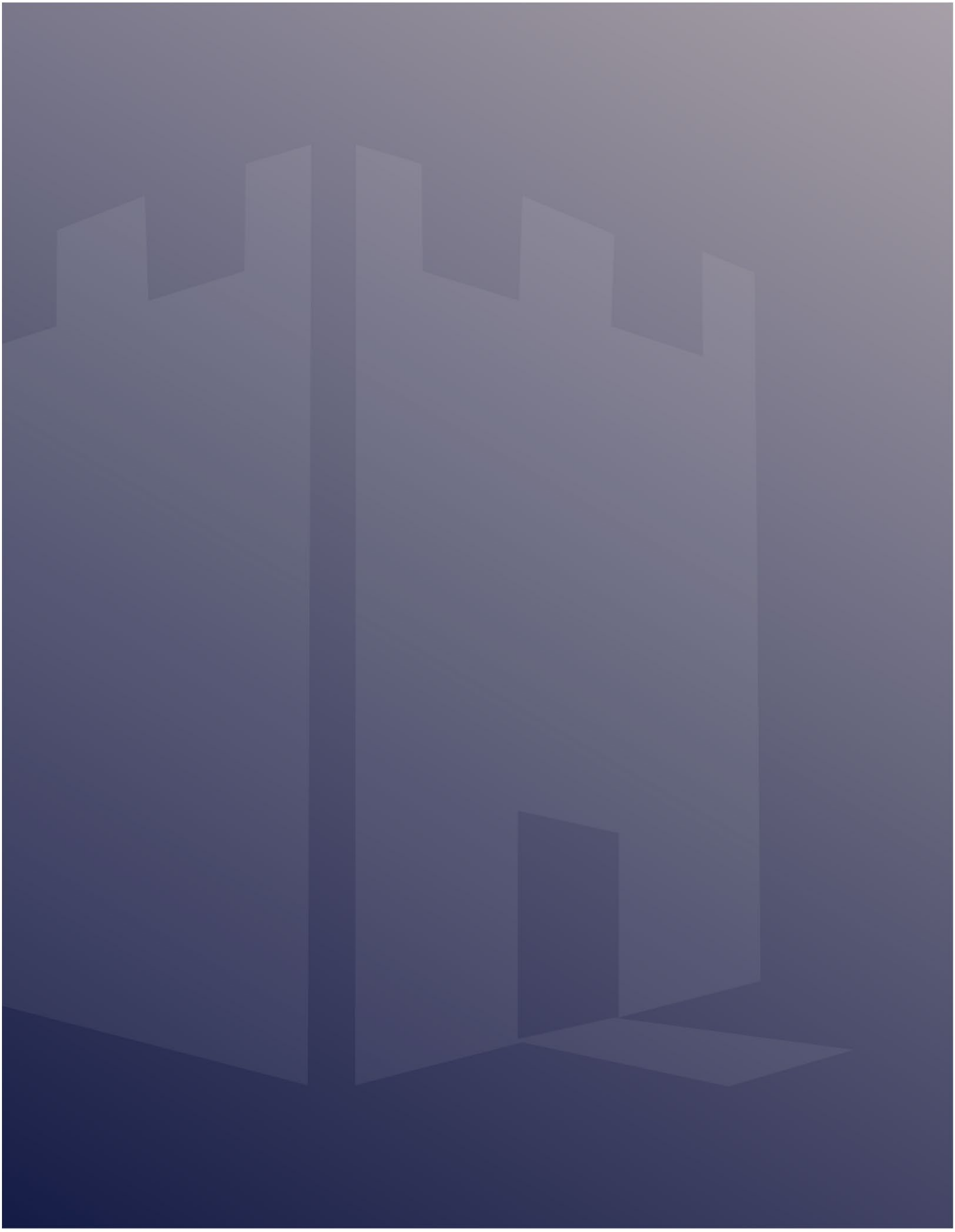
PONTEFRACT
ACADEMIES TRUST

Protection of Biometric Data Policy



Summary:

We collect and process biometric data in accordance with the relevant legislation and guidance to ensure the data and the rights of individuals are protected. We will treat the data collected with appropriate care.

This policy outlines the procedure each school follows when collecting and processing biometric data.

Author	Head of Governance		
Applies to: (please check as appropriate)	Staff ✓	Student ✓	Community ✓
Ratifying Committee(s):	Audit and Risk Committee		
Available on:	Compliance Library ✓	Website ✓	
Date of Approval:	13/10/2023		
Date of Next Formal Review: (ensure this is aligned to committee meeting dates)	13/10/2024		
Review Period:	Annual		
Status:	Non-contractual		
Owner:	**Pontefract Academies Trust**		
Version:	02		

Document Control

Date	Version	Action	Amendments
August 2022	01	New Policy	
September 2023	02	Reviewed	None

Contents

1. Statement of intent

Pontefract Academies Trust 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 the relevant legislation and guidance to ensure the data and the rights of individuals are protected. We will treat the data collected with appropriate care.

This policy outlines the procedure each school follows when collecting and processing biometric data.

2. Definitions

Biometric data is personal information, resulting from specific technical processing, 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.

An 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. Biometric recognition systems can use many kinds of physical or behavioural characteristics, such as those listed above.

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' biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.
- Storing students' biometric information on a database.
- Using students' 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 is personal data which the UK GDPR says is more sensitive, and so needs more protection. Where biometric data is used for identification purposes, e.g. through keystroke analysis, it is considered special category data.

3. Roles and responsibilities

The Audit & Risk Committee are responsible for reviewing this policy on an annual basis.

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

The Head of Governance 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 Trust will ensure 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 Trust is responsible for being able to demonstrate its compliance with the provisions outlined above.

5. Data protection impact assessments (DPIA's)

Prior to processing biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out. The Head of Governance will oversee and monitor the process of carrying out the DPIA.

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.
- Be reviewed frequently and kept updated.

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 Head of Governance will consult the DPO before the processing of biometric data begins.

The DPO will provide the Trust with a written response whether the risks are acceptable, or whether the school needs to take further action. In some cases, the DPO may advise the Trust not to carry out the processing. The Trust will adhere to any advice from the DPO.

6. 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 students' 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.

Prior to any biometric recognition system being put in place or processing students' biometric data, the school will take consent/non-consent from the admissions form parents complete.

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

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 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.

Where neither parent of a student 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 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.

Information available for 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.
- How the data will be stored.
- The parent's and the student's right to refuse or withdraw their consent.
- The school's duty to provide reasonable alternative arrangements for those students whose information cannot be processed.

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.

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

Where a student or their parents object, 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 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.

Where staff members or other adults use the school's biometric systems, 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 systems and can withdraw their consent at any time. Where this happens, and 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 systems, in line with the alternatives arrangements section of this policy.

7. Alternative arrangements

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

Where an individual objects to taking part in the school's biometric systems, 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, the student will be able to access funds by using a name lookup process where they tell their name to the lunch time staff and the amount is charged to that student's account, validated by photographic evidence, or by the issuance of a unique user code.

Any alternative arrangements implemented will ensure that steps are taken to minimise and mitigate any attempted abuse of the process.

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 parent, where relevant).

8. Data retention

Biometric data will be managed and retained in line with the Trust Information Policy. If an individual, including a student'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

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 systems will be managed in accordance with the Data and Cyber-security Breach Prevention and Management Plan.

10. Monitoring and review

The Audit & Risk Committee and Trust Board will review this policy on an annual basis.

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

Appendix A: Consent form for the use of biometric information

Consent form for the use of biometric information

Please complete this form to confirm whether you provide consent for the school to collect and use the following biometric information relating to you/your child:

- fingerprint

The school would like to use this information for the purpose of providing you/your child with access to funds to purchase school lunches.

Having read the guidance provided to me by the school, I (please tick your selection):

- **Do** consent to the processing of my/my child's biometric data ☐
- **Do not** consent to the processing of my/my child's biometric data ☐

For the person/parents that have provided consent

Please confirm that you have read and understood the following terms:

- I authorise the school to use my/my child's biometric information for the purpose specified above until either I/they leave the school or cease to use the system.
- I understand that I can withdraw my consent at any time.
- I understand that, if I wish to withdraw my consent, I must do so in writing and submit this to the school office.
- I understand that once I/my child ceases to use the biometric system, the school will securely delete my/my child's biometric information.

I confirm that I have read and understood the terms above ☐

For all parents/staff

Name of child/staff member:	
Name of parent/staff member:	
Signature:	
Date:	

Please return this form to the school office by the relevant date.