Ormiston Academies Trust

Ormiston Herman Academy
Biometrics policy

Policy version control

Policy type	Statutory and Mandatory
Author	Alexandra Coughlan, Data Protection Officer
Approved by	OAT Executive, February 2024
Approved by Trust Board	March 2024
Release date	March 2024
Review	Policies will be reviewed in line with OAT's internal policy schedule and/or updated when new legislation comes into force
Description of changes	▪ Updated to include reference to special category data policy

Contents

Ormiston Academies Trust 1
Ormiston Herman Academy Biometrics policy 1
Policy version control 1
Contents 2
1. Introduction 3
2. Scope and purpose 3
3. Legal framework 3
4. Definitions 4
5. Roles and responsibilities 4
6. Data protection principles 5
7. Data protection impact assessments (DPIAs) 5
8. Notification and consent 5
9. Alternative arrangements 7
10. Data retention 8
11. Breaches 8
12. Monitoring and review 8

1. Introduction

1.1. The Ormiston Academies Trust (referred to as "the trust" and any or all of its academies) collects and uses certain types of personal information about staff, pupils, parents, and other individuals who come in contact with its academies, in order to provide education and associated functions. The trust may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education, and safeguarding.

1.2. This policy is intended to ensure where we collect and process biometric data for the purposes above that we do so in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected.

1.3. This policy outlines the procedure the trust and its academies follow when collecting and processing biometric data in accordance with the United Kingdom General Data Protection Regulation (UK GDPR) and other related legislation.

1.4. This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, this policy will be reviewed and updated as necessary every twelve months.

2. Scope and purpose

2.1. The purpose of the document is to set out clearly how as a trust we meet our statutory obligation with regards to the curation and use of biometric data. The policy applies to the storage of all biometric data including the data of staff, pupils, and visitors and is reviewed by the trust on an annual basis.

2.2. All staff who are involved in storing data are trained on the content.

2.3. The policy should be read in conjunction with the following Ormiston Academies Trust policies.

- Data protection and freedom of information policy
- Records retention policy

3. Legal framework

3.1. 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
- United Kingdom General Data Protection Regulation (UK GDPR)
- DfE (2018) 'Protection of biometric information of children in Academies and colleges'

3.2. This policy operates in conjunction with the following academy policies:

- Data protection and freedom of information policy
- Special category data
- Records retention policy

4. Definitions

4.1. **Biometric data**: Personal information about an individual's physical or behavioural characteristics that can be used to identify that person. This can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

4.2. **Automated biometric recognition system**: a system which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (ie. electronically). Information from the individual is automatically compared with biometric information stored in the system to match with data stored about an individual.

4.3. **Processing biometric data:** includes obtaining, recording or holding biometric data or carrying out any operation on the data including disclosure, deletion, amendment or organization of the data.

4.4. **Special category data:** personal data which the GDPR says is more sensitive as defined in Article 9 of the UK GDPR. Biometric data used for identification purposes is defined by Article 9 as special category data.

5. Roles and responsibilities

5.1 The **executive body** of the trust is responsible for reviewing this policy on an annual basis.

5.2 The **academy principal** is responsible for ensuring the provisions in this policy are implemented consistently.

5.3 The **academy data protection lead** (DPL) is responsible for monitoring the academy's compliance with data protection legislation in relation to the use of biometric data.

5.4 The **data protection officer** (DPO) is responsible for advising on when it is necessary to undertake a data protection impact assessment (DPIA) in relation to the academy's biometric system(s) and for being the first point of contact for the ICO and for individuals whose data is processed by the academy and connected third parties.

6. Data protection principles

6.1. The academy processes all personal data, including biometric data, in accordance with the key principles set out in the UK GDPR. These principles are set out in section 3 of the Ormiston Academies Trust Data protection and freedom of information policy.

6.2. In addition to this the trust is always committed to ensuring that anyone dealing with personal data shall be mindful of the individual's rights under the law. These are explained in more detail in sections 11 to 13 of the Data Protection and Freedom of Information Policy.

7. Data protection impact assessments (DPIAs)

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

7.2. Requests for DPIA must be made using the OATnet form here: https://ormistonacademiestrust.sharepoint.com/sites/data-protection/SitePages/Data-Protection-Impact-Assessment.aspx

7.3. Further guidance on how to complete the request is available on the OATnet DPIA page.

7.4. Submission for a DPIA must include the upload of documentation from your service provider to clarify how they manage GDPR and Data Protection compliance.

7.5. The DPO will conduct the DPIA to:

- Assess the nature, scope, context, and purposes of the processing
- Assess necessity, proportionality, and compliance measures
- Identify and assess risks to individuals
- Identify any additional controls that may need to be applied to mitigate those risks

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

7.7. If a high risk is identified that cannot be mitigated by additional and reasonable controls, the DPO will consult the ICO before the processing of the biometric data begins.

7.8. The ICO will provide the academy with a written response and the academy will adhere to any advice provided in the response from the ICO.

8. Notification and consent

8.1. The academy must obtain consent for the processing of biometric data as required by Section 26 of the Protection of Freedoms Act 2012.

8.2. Where the academy uses pupils' biometric data as part of an automated biometric recognition system the academy will comply with the requirements of the Protection of Freedoms Act 2012.

8.3. Prior to any biometric recognition system being put in place or processing a pupil's biometric data, the academy will send the pupils' parents a parental notification and consent form for the use of biometric data.

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

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

8.6. Where the name of only one parent is included on the admissions register, the principal will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent.

8.7. The academy 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

8.8. Where neither parent of a pupil can be notified, 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

8.9. Where a parent disputes consent provided by the other parent consent will be deemed to have not been provided and both parents informed that this will be the case and reasonable alternative arrangements will be provided.

8.10. 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 pupils right to refuse or withdraw their consent
- The academy's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed

8.11. The academy 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

8.12. Parents and pupils can object to participation in the academy'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.

8.13. If a pupil objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the academy 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).

8.14. Pupils will be informed that they can object or refuse to allow their biometric data to be collected and used via a letter.

8.15. Where staff members or other adults use the academy's biometric system(s), consent will be obtained from them before they use the system.

8.16. Staff and other adults can object to taking part in the academy'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.

8.17. Reasonable alternative arrangements will be provided to any individual that does not consent to take part in the academy's biometric system(s), in line with section 9 of this policy.

9. Alternative arrangements

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

9.2. Where an individual objects to taking part in the academy'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 is used to pay for academy meals, the pupil may be able to use cash or a card for the transaction instead. Alternatively, a PIN may be provided where available.

9.3. 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).

10. Data retention

10.1. Biometric data will be managed and retained in line with Ormiston Academies Trust Records retention policy.

10.2. 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 academy's system.

11. Breaches

11.1. There are appropriate and robust security measures in place to protect the biometric data held by the academy. These measures will be detailed in any relevant DPIAs completed.

11.2. Any breach to the academy's biometric system(s) will be dealt with in accordance with the Ormiston Academies Trust Data protection and freedom of information policy.

12. Monitoring and review

12.1. The executive body of the trust will review this policy on an annual basis.

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