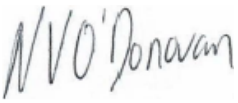
PROTECTION OF BIOMETRIC INFORMATION POLICY

Adopted by the Trustees of Leodis Academies Trust 5 December 2019

This policy applies to all members of Leodis Academies Trust (**Trust**). For the purposes of this policy, the term 'staff' means all members of staff within Leodis Academies Trust including permanent, fixed term and temporary staff. It also refers to governors, any third party representatives, agency workers and volunteers. All those who use or have access to the Trusts information must understand and adopt this policy and are responsible for ensuring the security of the information they use.

The Trustees have delegated responsibility to the Principal in each Academy for ensuring compliance and this policy within the day-to-day activities of their Academy.

Distribution
Leodis Academies Trust
Blackgates Primary Academy
East Ardsley Primary Academy
Hill Top Primary Academy
Westerton Primary Academy
Woodkirk Academy

Signed: … 

N O'Donovan
Chair of Trustees

CONTENTS PAGE

1. INTRODUCTION

1.1. The Trust is committed to protecting the personal data of all its students and staff; this includes any biometric data we may collect and process.

1.2. We will always 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 Trust follows when collecting and processing biometric data.

2. LEGAL FRAMEWORK

2.1. This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

2.1.1. Protection of Freedoms Act 2012.

2.1.2. Data Protection Act 2018.

2.1.3. General Data Protection Regulation (GDPR).

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

2.2. This policy operates in conjunction with the following Trust policies:

2.2.1. Data Protection Policy.

2.2.2. Records Management Policy.

3. DEFINITIONS

3.1. **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.

3.2. **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.

3.3. **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:

3.3.1. Recording students' biometric data, for example taking measurements from a fingerprint via a fingerprint scanner.
3.3.2. Storing students' biometric information on a database.
3.3.3. Using students' biometric data as part of an electronic process, for example by comparing it with biometric information stored on a database to identify or recognise students.

3.4. **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.

4. ROLES AND RESPONSIBILITIES

4.1. The Trustees are responsible for renewing this policy on an annual basis.

4.2. The Principal of each Academy within the Trust is responsible for ensuring the provisions in this policy are implemented consistently.

4.3. The Data Protection Officer is responsible for:

4.3.1. Monitoring the Trust's compliance with data protection legislation in relation to the use of biometric data.
4.3.2. Advising on when it is necessary to undertake a data protection impact assessment (DPIA) in relation to the Trust's biometric system(s).
4.3.3. Being the first point of contact for the ICO and for individuals whose data is processed by the Academy and connected third parties.

5. DATA PROTECTION PRINCIPLES

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

5.2. The Trust ensures biometric data is:

5.2.1. Processed lawfully, fairly and in a transparent manner.
5.2.2. Only collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
5.2.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
5.2.4. Accurate and, where necessary, kept up-to-date, and that reasonable steps are taken to ensure inaccurate information is rectified or erased.
5.2.5. 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.
5.2.6. 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.

5.3. As the data controller, the Trust is responsible for being able to demonstrate its compliance with the provisions outlined in 5.2.

6. DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

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

6.2. The Data Protection Officer will oversee and monitor the process of carrying out the DPIA.

6.3. The DPIA will:

6.3.1. Describe the nature, scope, context and purposes of the processing.
6.3.2. Assess necessity, proportionality and compliance measures.

6.3.3. Identify and assess risks to individuals.
6.3.4. Identify any additional measures to mitigate those risks.

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

6.5. If a high risk is identified that cannot be mitigated, the Data Protection Officer will consult the ICO before the processing of the biometric data begins.

6.6. The ICO will provide the Trust with a written response (within eight weeks or 14 weeks in complex cases) advising whether the risks are acceptable, or whether the Trust needs to take further action. In some cases, the ICO may advise the Trust to not carry out the processing.

6.7. The Trust will adhere to any advice from the ICO.

7. NOTIFICATION AND CONSENT

7.1. Where the Trust uses students' biometric data as part of an automated biometric recognition system (for example, using students' fingerprints to receive food and drink instead of paying with cash), the Trust will comply with the requirements of the Protection of Freedoms Act 2012..

7.2. Prior to any biometric recognition system being put in place or processing a student's biometric data, the Trust will send the student's parents a Parental Notification and Consent Form for the use of Biometric Data.

7.3. Written consent will be sought from at least one parent of the student before the Trust collects or uses a student's biometric data.

7.4. The name and contact details of the student's parents will be taken from the Trust's admission register.

7.5. 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.

7.6. The Trust does not need to notify a particular parent or seek their consent if it is satisfied that:

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

7.7. Where neither parent of a pupil 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:

7.7.1. If a student is being 'looked after' by the Local Authority or is accommodated or maintained by a voluntary organisation, the Local Authority or voluntary organisation will be notified and their written consent obtained.
7.7.2. 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.

7.8. Notification sent to parents and other appropriate individuals or agencies will include information regarding the following:

7.8.1. Details about the type of biometric information to be taken.
7.8.2. How the data will be used.
7.8.3. The parent(s) and the student's right to refuse or withdraw their consent.
7.8.4. The Trust's duty to provide reasonable alternative arrangements for those students whose information cannot be processed.

7.9. The Trust will not process the biometric data of a student under the age of 18 in the following circumstances:

7.9.1. The student (verbally or non-verbally) objects or refuses to participate in the processing of their biometric data.
7.9.2. No parent or carer has consented in writing to the processing.
7.9.3. A parent has objected in writing to such processing, even if another parent has given written consent.

7.10. Parents and students can object to participation in a biometric system within the Trust 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.

7.11. If a student objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the individual Academy 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).

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

7.13. Where staff and other adults use a biometric system within the Trust, consent will be obtained from them before they use the system.

7.14. Staff and other adults can object to taking part in the biometric system(s) within the Trust 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.

7.15. Alternative arrangements will be provided to any individual that does not consent to take part in the biometric systems within the Trust, in line with Section 8 of this policy.

8. ALTERNATIVE ARRANGEMENTS

8.1. Parents, students, staff and other relevant adults have the right to not take part in the Trust's biometric system.

8.2. Where an individual objects to taking part in the Trust's biometric system, reasonable alternative arrangements will be provided that allow the individual to access the relevant service, for example where a biometric system uses student's fingerprints to pay for food and drink, the student will be able to use a card for the transaction instead.

8.3. 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 student's parents, where relevant).

9. DATA RETENTION

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

9.2. If an individual (or a student's parent, where relevant) withdraws their consent for their/their son/daughter's biometric data to be processed, it will be erased from the Trust's system.

10. BREACHES

10.1. There are appropriate and robust security measures in place to protect the biometric data held by the Trust. These measures are detailed in the Trust's Data Protection Policy.

10.2. Any breach to the Trust's biometric system will be dealt with in accordance with the Trust's Data Protection Policy.

11. MONITORING AND REVIEW

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