DND Learning Trust

Durham and Newcastle Diocesan Learning Trust (DNDLT)
Company Number 10847279

Protection of Biometric Data Policy

Every child matters and no child is ever left behind..."

"Let the little children come to me, and do not stop them;
for it is to such as these that the kingdom of God belongs."
Luke 18:15-17

Policy Reviewed and Adopted by Board of Directors: as part of Staff Handbook Sept 2025
Version:4
Date of Next Review: Annual (as part of Staff Handbook review)
Responsible Officer: COO

Vision Statement

"Every child matters and no child is ever left behind"

Let the children come to me, and do not stop them; for it is to such as these that the kingdom of God belongs.

Luke +

At the DNDLT we believe everyone in our Trust is a child of God, adults and children alike. Every individual and every school matters, all are valued and celebrated, and no one should be left behind.

As a Diocesan Trust of the Dioceses of Newcastle and Durham we are here to serve children, and schools of all faiths and none. We welcome both Church of England and Community Schools to join us to serve our communities in the North East of England as part of our Trust family whilst remaining unique and distinct within their local context.

The Durham and Newcastle Diocesan Learning Trust is a place where we strive for the best outcomes for our children and staff. We work hard to achieve equity and flourishing for everyone. We want our staff and children to feel valued and celebrated given the opportunity to innovate and reach their full potential. We want our schools to be at the heart of their communities serving them in the way they know best, knowing they will be supported, encouraged and affirmed by a dedicated and specialist team.

1. This policy

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

1.2. The Trust may collect and process biometric data in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected.

1.3. This policy outlines the procedures the trust follows when collecting and processing biometric data.

1.4. This policy does not form part of any employee's contract of employment.

1.5. The Trust has overall responsibility for this policy, including keeping it under review.

1.6. This policy has due regard to all relevant legislation and guidance including, but not limited to the Protection of Freedoms Act 2012; Data Protection Act 2018; General Data Protection Regulation (GDPR); DfE (2022) 'Protection of biometric information of children in academy's and colleges' and the Trust's Data Protection Policy.

2. Definitions

2.1. The following definitions apply in this policy:-

2.1.1. "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.

2.1.2. "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.

2.1.3. "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:-

2.1.3.1. Recording pupils/staff biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.

2.1.3.2. Storing pupils/staff biometric information on a database.

2.1.3.3. Using pupils/staff 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.

2.1.4. "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.

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

3. General Principles

3.1. The Trust will ensure biometric data is:

3.1.1. Processed lawfully, fairly and in a transparent manner.

3.1.2. Only collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.

3.1.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

3.1.4. Accurate and, where necessary, kept up-to-date, and that reasonable steps are taken to ensure inaccurate information is rectified or erased.

3.1.5. 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.

3.1.6. 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.

4. Data Protection Impact Assessment

4.1. Prior to processing biometric data or implementing a system that involves processing biometric data, a Data Protection Impact Assessment (DPIA) will be carried out, which will:-

4.1.1. Describe the nature, scope, context and purposes of the processing.

4.1.2. Assess necessity, proportionality and compliance measures.

4.1.3. Identify and assess risks to individuals.

4.1.4. Identify any additional measures to mitigate those risks.

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

4.3. If a high risk is identified that cannot be mitigated, the DPO will consult the Information Commissioner's Officer (ICO) before the processing of the biometric data begins. The Trust will adhere to any advice from the ICO.

5. Consent

5.1. Please note that the obligation to obtain consent for the processing of biometric information of individuals 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.

5.2. Where the Trust uses pupil and staff biometric data as part of an automated biometric recognition system (e.g. using pupils' fingerprints to receive school lunch meals instead of paying with cash), the Trust will comply with the requirements of the Protection of Freedoms Act 2012.

5.3. In respect of pupils, written consent will be sought from at least one parent with parental responsibility for the pupil before the Trust collects or uses a pupil's biometric data.

5.4. The Trust will not process the biometric data of an individual under the age of 18 in the following circumstances:

5.4.1. They (verbally or non-verbally) object or refuse to participate in the processing of their biometric data;

5.4.2. No parent or carer has consented in writing to the processing;

5.4.3. A parent has objected in writing to such processing, even if another parent has given written consent.

5.5 The name and contact details of pupils' 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.

5.6 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.

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
- How the data will be stored
- 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

5.7 Individuals (or their parents if under 18) can object to participation in the Trust'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.

5.8 Where a pupil objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the trust 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).

5.9 Where staff members or other adults use the trust'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 trust'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.

5.10 Where an individual objects to taking part in the trust's biometric system(s), reasonable alternative arrangements will be provided as set out below.

6. Alternative arrangements

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

6.2. 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 pupil's fingerprints to pay for school meals, the pupil will be able to use cash for the transaction instead.

6.3. 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).

7. Storage and data retention

7.1. Biometric data will be managed and retained in line with the school's data retention schedule/records management policy.

7.2. The school will only store and process biometric information for the purpose for which it was originally obtained and consent provides.

7.3. If an individual, including a pupil's parent, where relevant, withdraws their consent for their or their child's biometric data to be processed, it will be erased from the school's system.

8. Further information

8.1. Department for Education's 'Protection of Biometric Information of Children in Schools–

https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools