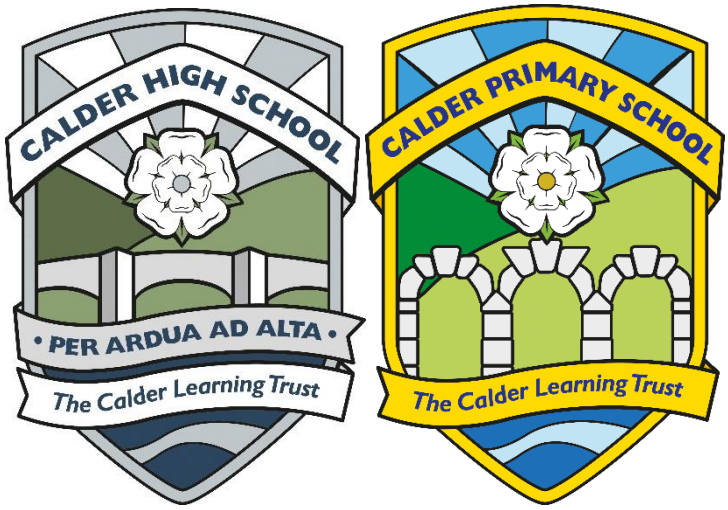

Calder Learning Trust

Protection of Biometric Information Policy

2023

Last reviewed:	January 2023
Next review due by:	January 2024

The Calder Learning Trust 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.

What is Biometric Data?

Biometric data means 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.

Schools and academies that use pupils' biometric data must treat the data collected with appropriate care and must comply with the data protection principles as set out in the General Data Protection Regulation 2018.

The Information Commissioner considers all biometric information to be personal data as defined by the General Data Protection Regulation 2018; this means that it must be obtained, used and stored in accordance with the Regulation.

Personal data used as part of an automated biometric recognition system must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.

The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data in schools, academies and colleges when used as part of an automated biometric recognition system.

Schools and academies must ensure that the parent/carer of each pupil is informed of the intention to use the pupil's biometric data as part of an automated biometric recognition system. Parents/carers must be advised that alternative methods to biometric scanning are available for processing identity if required.

The written consent of the parent/carer or the pupil, where the pupil is deemed to have the capacity to consent, must be obtained before the data is taken from the pupil and processed within the biometric recognition system. In no circumstances can a pupil's biometric data be processed without written consent.

Schools and academies must not process the biometric data of a pupil where:

a) the pupil (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;

b) a parent or pupil has not consented in writing to the processing; or

c) a parent or pupil has objected in writing to such processing, even if another parent has given written consent.

Schools and academies must provide reasonable alternative means of accessing the services to those pupils who will not be using an automated biometric recognition system.

Biometric Data and Processing

What Is an Automated Biometric Recognition System?

An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e.

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

What Does Processing Data Mean?

'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

a) recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;

b) storing pupils' biometric information on a database system; or

c) using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise pupils.

Who Is Able to Give Consent?

The Data Protection Act gives pupils rights over their own data when they are considered to have adequate capacity to understand. Most pupils will reach this level of understanding at around age 13. For this reason, for most pupils in a secondary school, it will normally be up to the individual pupil to decide whether or not to provide biometric data. Where the school or academy considers that the pupil does not have the capacity, or they are under the age of 13, parents/carers will be asked to provide written consent.

Alternative to Biometric

The school or academy will provide an alternative to biometric scanning for any parent/pupil objecting to the processing of biometric data.

Length of Consent

The original written consent is valid until such time as it is withdrawn. However, it can be overridden, at any time either parent/carer or the pupil themselves objects to the processing (subject to the parent's/carer's objection being in writing). When the student leaves the school or academy, their biometric data will be securely removed from the academy's biometric recognition system.

Associated Resources

DfE guidelines for schools on communicating with parents and obtaining consent:

https://www.gov.uk/government/publications/dealing-with-issues-relating-toparental-responsibility.

ICO guide to data protection:

http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx

ICO guidance on data protection for education establishments:

http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx

This policy will be reviewed by The Governing Body or Trustees to ensure that it meets legal requirements and reflects best practice.