Extend Learning
Academies Network

Protecting Children's Biometric Data Policy

Version:	4.1	
Written by:	ELAN executive team	
Reviewed by:	ELAN Board	Date: 06.02.2024
Approved by:	Name: Rosemary Carr Signed by: Rosemary Carr Chair of the Board	Date: 06.02.2024
Adopted by Academies:	Banwell Primary School Bournville Primary School Locking Primary School Mead Vale Primary School Mendip Green Primary School Milton Park Primary School Oldmixon Primary School Walliscote Primary School Windwhistle Primary School	
Review:	Annually	
Next Review Due By:	November 2024	

Document Control
Document Information

	Information
Document Name	Protecting children's biometric data policy
Document Author	Data protection officer (DPO)
Document Approval	Data protection officer (DPO)
Document Status	Version 4.1
Publication Date	February 2024
Review Date	November 2024
Distribution	Website/General

Version Control

Version	Issue Date	Amended by	Comments
1.0	12/02/2020	Data protection officer	New trust policy
2.0	March 2021	Data protection officer	Annual review, no updates required.
3.0	July 2022	Data protection officer	Annual review, updated with DfE 2022 guidance.
4.0	October 2023	Data protection officer	Annual review – updating incorrect numbering in section 2.
4.1	Feb 2024	Data protection officer	Inclusion of data impact assessment section 6.

Contents

1 Statement of intent

Extend Learning Academies Network (ELAN) and the schools that make up the multi academy trust (MAT) aims to ensure that all personal data collected about employees, pupils, parents, governors, visitors, contractors, suppliers and other individuals in any way lawfully associated with ELAN or any of its schools, is collected, stored and processed in accordance with the Data Protection Act 2018 (DPA), UK General Data Protection Regulation and the Protection of Freedoms Act 2012.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Any reference to ELAN within this policy applies to any or all of its schools and central locations as appropriate.

This policy should be read in conjunction with ELAN's privacy notices for pupils, employees, governors and suppliers, contractors and volunteers, and the data protection policy.

2 Introduction – key points

Schools that use pupils' biometric data (see point 3 below) must treat the data collected with appropriate care and must comply with the data protection principles as set out in the Data Protection Act 2018 (DPA), UK General Data Protection Regulation and the Protection of Freedoms Act 2012.

Where the data is to be used as part of an automated biometric recognition system (see point 4), schools must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.

Schools must ensure that the parent/carer of each child is informed of the intention to use the child's biometric data (see point 2) as part of an automated biometric recognition system.

The written consent of the parent/carer or the child, where the child is deemed to have the capacity to consent (see below), must be obtained before the data is taken from the child and used (i.e. 'processed' – see point 4). In no circumstances can a child's biometric data be processed without written consent.

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

- the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data
- a parent or pupil has not consented in writing to the processing or
- a parent or pupil has objected in writing to such processing, even if another parent has given written consent.

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

3 What is biometric data?

Biometric data means personal information resulting from specific technical processing relating to the individual's physical, psychological or behavioural characteristics which allow or confirm the unique identification of that person, such as facial images, voice recognition or fingerprints.

The Information Commissioner considers all biometric information to be personal data as defined by the UK General Data Protection Regulations.

This means that it must be obtained, used and stored in accordance with that Regulation.

The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data in schools and colleges when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the Data Protection Act 2018 and the UK General Data Protection regulations.

4 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).

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 in point 3 above.

5 What does data processing 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:

- recording pupil's biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner
- storing pupils' biometric information on a database system; or
- 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.

6 Data protection impact assessments (DPIAs)

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

The Data Protection Officer (DPO) 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

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 DPO will consult the ICO before the processing of the biometric data begins.

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

ELAN will adhere to any advice from the ICO.

7 Who is able to give consent?

In order to comply with the requirements of the Protection of Freedoms Act 2012, schools must notify each parent, carer/legal guardian of the child of their intention to process the child's biometric information, and that the parent may object at any time to the processing of the information.

A child's biometric information must not be processed unless at least one parent of the child consents, and no parent of the child has withdrawn his or her consent, or otherwise objected, to the information being processed. In addition, a pupil's objection or refusal, overrides any parental consent to the processing, therefore any biometric data must not be processed.

The Protection of Freedoms Act 2012 defines a parent to mean "a parent of the child and any individual who is not a parent of the child but who has parental responsibility for the child". Practically it would be person(s) with parental responsibility for the child, be it birth, adoptive or an appointed body, who a school would notify and seek consent from to process personal biometric data. Any one parent could give or withhold consent.

Where a child is looked after and is subject to a care order in favour of the local authority or the local authority provides accommodation for the child within the definition of section 22(1) of the Children Act 1989, a school would not be required to notify or seek consent from birth parents.

If a pupil under the age of 18 objects or refuses to participate (or to continue to participate) in activities that involve the processing of their biometric data, the school must ensure that the pupil's biometric data is not taken/used as part of a biometric recognition system. A pupil's objection or refusal overrides any parental consent to the processing.

8 Length of consent

The original written consent is valid until such time as it is withdrawn.

However, it can be overridden, at any time if either parent or the child themselves objects to the processing (subject to the parent's objection being in writing).

When the pupil leaves the school, their biometric data will be securely removed from the school's biometric recognition system.

9 Alternative to biometric

Any school using a biometric system will offer an alternative to biometric scanning and any pupil objecting to the processing of their biometric data will be informed of the alternative provision.

10 Policy Review

The Data Protection Officer (DPO) is responsible for monitoring and reviewing this policy.

The policy will be reviewed annually.

The next scheduled review date for this policy is November 2024.

11 Appendix 1 - Biometric Consent form (parent/carer)

Pupil name: …….

Please sign below if you consent to ……primary school on behalf of the Extend Learning Academies Network (ELAN) taking and using information from your son/daughter's fingerprint as part of an automated biometric recognition system.

This biometric information will be used by the school/ELAN for the purpose of

……

In signing this form, you are authorising the school/ELAN to use your childs's biometric information for this purpose until they either leave the school/ELAN or ceases to use the system.

If you wish to withdraw your consent at any time, this must be done so in writing and sent to the headteacher.

Once your child ceases to use the biometric recognition system, their biometric information will be securely deleted by the school/ELAN.

Parent consent:

Having read the above guidance information, I give consent to information from the fingerprint of my child being taken and used by the school/ELAN for use as part of an automated biometric recognition system for the purpose of

…….

I understand that I can withdraw this consent at any time in writing.

Parent name: …….

Signature: ……

Date: ……