Protection of Biometric Information of Children in Schools and Colleges

Version 1

N.B. This policy is awaiting consultation with relevant recognised trade unions.

This policy applies to all NCLT institutions.

CONTENTS

Paragraph Number	Heading	Page Number
1.0	Introduction	3
2.0	Legal Context	3
3.0	Definitions	3
4.0	Roles and Responsibilities	4
5.0	Data Protection Principles	4
6.0	Data Protection Impact Assessments (DPIAs)	5
7.0	Notification and Consent	5
8.0	Alternative Arrangements	7
9.0	Data Retention	7
10.0	Data Breaches	8
11.0	Monitoring and Review	8
Appendix	Wingfield Admissions Form	8

1.0 Introduction

1.1 New Collaborative Learning Trust is committed to protecting the personal data of all its pupils and staff, this includes any biometric data collected and processed.

1.2 The Trust collects and processes 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 procedure the Trust follows when collecting and processing biometric data.

2.0 Legal Context

2.1 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
- UK General Data Protection Regulation (UK GDPR)
- Department for Education (DfE) (2018) Protection of biometric information of children in schools and colleges

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

- Data Protection Policy
- Personal Data Breach Policy
- Trust Data Retention Schedule

3.0 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:

- Recording pupils' biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.
- Storing pupils' biometric information on a database.
- Using pupils' 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.

3.4 **Special category data:** Personal data which the UK GDPR says is more sensitive, and so needs more protection – where biometric data is used for identification purposes, it is considered special category data.

4.0 Roles and Responsibilities

4.1 The Trust Executive Team and the Board of Directors are responsible for reviewing this policy on a bi-annual basis.

4.2 The Headteacher/Principal at each institution within the Trust is responsible for ensuring the provisions of this policy are implemented consistently.

4.3 The Data Protection Officer (DPO) is responsible for:

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

5.0 Data Protection Principles

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

5.2 The Trust ensures biometric data is:

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

- 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.

- 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 the UK GDPR.

6.0 Data Protection Impact Assessments (DPIAs)

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

6.2 The DPO will oversee and monitor the process of carrying out the DPIA.

6.3 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.

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 DPO 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.

7.0 Notification and Consent

7.1 The obligation to obtain consent for the processing of biometric information of children under the age of 18 is not imposed by the Data Protection Act 2018 or the UK GDPR. Instead, the consent requirements for biometric information is imposed by section 26 of the Protection of Freedoms Act 2012.

7.2 Where the Trust uses pupils' or students' biometric data as part of an automated biometric recognition system (e.g. using pupils' fingerprints to receive school meals

instead of paying with cash), the Trust will comply with the requirements of the Protection of Freedoms Act 2012.

7.3 Prior to any biometric recognition system being put in place or processing a child's biometric data, the Trust will seek to notify and gain consent from parents/carers for any child under the age of 18.

7.4 Reasonable steps will be made to ensure each parent or carer of a pupil or student is notified.

7.5 In the case of school information, the name and contact details of the pupil's parents/carers will be taken from the school's admission register.

7.6 Where the name of only one parent/carer is available, the Headteacher/Principal will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent/carer.

7.7 Written consent will be sought from at least one parent/carer of the pupil before the school collects or uses a pupil's biometric data. In the case of Wingfield, this will be done through the school's Admission Form (see Appendix 1).

7.8 The Trust will not need to notify a particular parent or carer, or seek their consent if the Trust is satisfied that:

- The parent/carer cannot be found, for example, their whereabouts or identity is not known.
- The parent/carer lacks the mental capacity to object or to consent.
- The welfare of the child requires that a particular parent/carer is not contacted, for example where a child has been separated from an abusive parent/carer who is not to be informed of the child's whereabouts.
- Where it is otherwise not reasonably practicable for a particular parent/carer to be notified or for their consent to be obtained.

7.9 Where neither parent/carer of a child can be notified for any of the reasons set out in 7.8, consent will be sought from the following individuals or agencies as appropriate:

- If a child is being 'looked after' by the Local Authority (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 child and written consent will be obtained from at least one carer before the child's biometric data can be processed.

7.10 Notification sent to parents/carers 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/carer's and the pupil's right to refuse or withdraw their consent.
- The Trust's duty to provide reasonable alternative arrangements for any child whose information cannot be processed (see section 8).

7.11 The Trust will not process the biometric data of a child under the age of 18 in the following circumstances:

- The child (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/carer has objected in writing to such processing, even if the other parent/carer has given written consent.

7.12 The child and/or their parents/carers 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 child that has already been captured will be deleted.

7.13 If specific biometric data beyond pupil/student photographs is required, e.g. fingerprints, parents or carers will be encouraged to discuss this with the child and then provide or refuse consent.

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

7.15 Staff and other adults can object to taking part in the school'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.

7.16 Alternative arrangements will be provided to any individual that does not consent to take part in the school's biometric system(s), in line with section 8 of this policy.

8.0 Alternative Arrangements

8.1 Parents/carers, pupils, students, staff members and other relevant adults have the right to not take part in the school's biometric system(s).

8.2 Where an individual objects to taking part in the Trust'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 uses pupil's fingerprints to pay for school meals, the pupil will be issued with a five digit pin number to access their dinner account.

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 child's parents or carers, where relevant).

9.0 Data Retention

9.1 Biometric data will be managed and retained in line with the Trust's Retention Schedule.

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

10.0 Data 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 IT Security Standards Policy.

10.2 A Data Sharing Agreement must be in place for any third parties processing biometric information on behalf of the Trust. This agreement must set out the security measures in place, and the process to be followed in the event of a data breach.

10.3 All breaches involving personal data are dealt with through the Trust's Personal Data Breach Policy.

10.4 Any breach to the Trust's biometric system(s) affecting personal data will be dealt with in accordance with the Personal Data Breach Policy.

11.0 Monitoring and Review

11.1 The Trust Executive Team and the Board of Directors will review this policy on a biannual basis.

11.2 Any changes to this policy will be communicated to all staff, parents/carers and pupils or students.

Appendix A

Wingfield Academy - Admissions Form 2021

Parental consent for biometric data recording and storage

Fingerprints scans & biometric data – we operate a fingerprint system for meals, which has many advantages, CRB Cunninghams Education Solutions operate this system on behalf of R.M.B.C our catering suppliers. It saves your child from carrying cash every day as you can pay online and you can be confident that they are spending money on meals and not in the local shop. Pupils have their fingerprint registered on the system, which is then translated into letters and numbers. The letters and numbers are then used by the system to identify the child, the fingerprint is then discarded and the letters and numbers cannot be reinterpreted back into a fingerprint image.

Please sign below if you agree to the use of biometric data of your child for cashless catering purposes.

Signed …… Print name ……

Policy Status			
Policy Lead (Title)	Trust Data Protection Officer	**Review Period**	Annually
Reviewed By	Trust Executive Team/ Board of Directors	**Equality Impact Assessment Completed (Y/N)**	N

POLICY AMENDMENTS					
Version	**Approval Date**	**Page No./Paragraph No.**	**Amendment**	**Audience**	**Plan for Communicating Amendments**
Version 1	TET 09/11/2021 BoD 13/12/2021	Policy created		Trust staff, students/pupils, parents	Website, email