CRAMLINGTON LEARNING VILLAGE

BIOMETRIC DATA POLICY

Policy reviewed and adopted by Trustees	**May 2022**
Version	**2021-2022**
Approved By	**Standards and Outcomes Committee**
Date of next review	**May 2024**
Responsible Officer	**Richard Majer, Data Manager**

Biometric Data Policy

1. Aims

Our school aims to ensure that personal biometric data collected about staff and pupils, is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

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

2. Legislation and guidance

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

In addition, this policy complies with our funding agreement and articles of association.

3. What is biometric data?

3.1 Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic data.

3.2 The ICO considers all biometric information to be sensitive personal data as defined by the GDPR; this means that it must be obtained, used and stored in accordance with that Regulation.

3.3 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 GDPR.

4. Roles and responsibilities

This policy applies to the student body and to all staff employed by our school. Staff who are engaged in the collection, handling and storage of biometric information, and to external organisations or individuals working on our behalf must comply with this policy or they may face disciplinary action.

4.1 Governing body

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

4.2 Data protection officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO is also the first point of contact for individuals whose biometric data the school processes, and for the ICO.

Our DPO is Ken Brechin, Deputy Headteacher and is contactable via kbrechin@cramlingtonlv.co.uk

4.3 Data Controller

Cramlington Learning Village is the data controller for the purposes of student and staff biometric data. The Data Manager (Richard Majer) leads on facilitating the collection, processing and storage of biometric data.

4.4 Headteacher

The Co-Headteachers act as the representative of the data controller on a day-to-day basis.

4.5 All staff

Staff are responsible for:

- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If there has been a data breach

5. Biometric data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles for the collection, use and storage of biometric information.

6. The biometric recognition system at CLV

We use pupils' biometric data as part of an automated biometric recognition system, with pupils using fingerprints to receive school dinners instead of paying with cash, or a prepaid card. We comply with the requirements of the Protection of Freedoms Act 2012.

6.1 Parents/carers will be notified before their child first takes part in the biometric recognition process. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

6.2 Parents/carers and pupils over 13 years of age have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

6.3 Parents/carers and pupils over 13 years of age can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

6.4 As required by law, if a pupil over 13 years of age refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

6.5 Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

6.6 Once consent has been received, students will have their fingerprint scanned, which is then turned into a unique digital code. The academy does not store any visual record of the student fingerprints.

7. Disposal of records

When students or staff leave the school, or withdraw consent, the digital code is deleted promptly and securely. This information is not retained like other student information, which is stored, retained and then disposed of as per the data retention policy.

8. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedures set out in the data retention policy

9. Training

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

10. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every two years and shared with the full governing body.

Associated Resources

- ICO guide to data protection https://ico.org.uk/for-organisations/guide-to-data-protection/

- ICO guidance on data protection for education establishments (https://ico.org.uk/for-organisations/in-your-sector/education/)
- British Standards Institute guide to biometrics (https://shop.bsigroup.com/Browse-By-Subject/Biometrics/)