Cleaswell Hill School

Protection of Biometric Information Policy

Date Adopted:	Spring term 2020 (Tuesday 17 March 2020)
Date reviewed:	Spring term 2021
Date of Next Review:	LA directed

Either This policy outlines the procedure the school will follow if a decision is made to collect and process biometric data. It will also cover how school will ensure the data and the rights of individuals will be protected.

Or: This policy outlines the procedure the school follows when collecting and processing biometric data and toensure the data and the rights of individuals are protected

Definitions:

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.* (DfE March 2018)

An automated biometric recognition system is *A system which 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.* (DfE March 2018)

Roles and responsibilities

The governing board is responsible for:

- Reviewing this policy on an annual basis.

The headteacher is responsible for:

- Ensuring the provisions in this policy are implemented consistently.

The data protection officer (DPO) is responsible for:

1. Monitoring the school's compliance with data protection legislation in relation to the use of biometric data.
2. Advising on when it is necessary to undertake a data protection impact assessment (DPIA) in relation to the school's biometric system(s).
3. Being the first point of contact for the ICO and for individuals whose data is processed by the school and connected third parties.
4. The school's DPO is Susan Mitchell.

Principles

Cleaswell Hill School undertakes to

1. Process all personal data, including biometric data, in accordance with the key principles set out in the General Data Protection Regulation (GDPR) and in line with those policies the school has adopted in relation to GDPR
2. Treat the data collected with appropriate care and comply with the data protection principles as set out in the GDPR 2018.
3. Where we will use the data as part of an automated biometric recognition system, we will comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.
4. We will ensure that each parent of a child is notified of the school's intention to use the child's biometric data as part of an automated biometric recognition system.
5. Obtain the written consent of at least one parent before the data is taken from the child and used i.e.: 'processed'. This applies to all pupils in school under the age of 18. In addition we undertake to consult the child if they are over the age of 13 and not to collect or process data if this is against the wishes of the child or if a parent has objected in writing to such processing, even if another parent has given written consent.
6. Provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

Data protection impact assessments (DPIAs)

1. Prior to implementing any system that involves processing biometric data, a DPIA will be carried out.
2. The DPO will oversee and monitor the process of carrying out the DPIA.
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.
4. When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered.
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. The ICO will provide the school with a written response (within eight weeks or 14 weeks in complex cases) advising whether the risks are acceptable, or whether the school needs to take further action. In some cases, the ICO may advise the school to not carry out the processing.
7. The school will adhere to any advice from the ICO.