Protection of Biometric Information Policy

Date Adopted: January 2022
Date reviewed:
Date of Next Review: January 2024

1. **The Policy**

1.1 This Protection of Biometric Information Policy (the "**Policy**") outlines the procedure the School follows when collecting and processing Biometric Data to ensure the data and the rights of individuals are protected and the collection and processing of Biometric Data complies with Data Protection Legislation and guidance.

1.2 The Policy has been prepared in accordance with relevant legislation and guidance, including but not limited to:

1.2.1 Protection of Freedoms Act 2012;

1.2.2 General Data Protection Regulation ((EU) 2016/279)("**GDPR);**

1.2.3 Data Protection Act 2018 ("**DPA"**); and

1.2.4 The Department or Education "Protection of biometric information of children in schools and colleges" - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/692116/Protection_of_Biometric_Information.pdf (the "**Guidance**"),

as updated and / or amended from time to time.

2. **Definitions:**

Within this Policy the following words / terms shall have the following definitions:

Automated Biometric Recognition System: 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 Data stored in the system to see if there is a match in order to recognise or identify the individual.

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.

Data Protection Legislation: means all applicable data protection in force from time to time in the UK including (but not limited to) the General Data Protection Regulation ((EU) 2016/679) ('**GDPR**') and the Data

Protection Act 2018 ('**DPA'**) relating to Personal Data, and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data.

Personal Data: means any data which relates to a living individual who can be identified including Special Category Data.

Processing of Biometric Data: 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 Biometric Data when:

a. recording pupils' Biometric Data, for example, taking measurements from a fingerprint via a fingerprint scanner;

b. storing pupils' Biometric Data on a database system; or

c. using that Biometric 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.

Special Category Personal Data: Personal Data as defined within GDPR and / or DPA as being more sensitive, and therefore in need of greater more protection, including Biometric Data used for identification purposes.

3. Policy Management

3.1 The School's Governing Body board shall ensure this Policy is reviewed and amended (as appropriate) less than annually.

3.2 The School's headteacher shall ensure the provisions in this Policy are implemented consistently by all School staff, agents and volunteers.

3.3 The School's Data Protection Officer ("**DPO**") shall:

3.3.1 monitor the School's compliance with Data Protection Legislation in relation to the use of Biometric Data;

3.3.2 advise the School in relation to the necessity to undertake a Data Protection Impact Assessment ("**DPIA"**) in relation to the School's Automatic Biometric Recognition System(s); and

3.3.3 be the first point of contact for the Information Commissioners Office ("**ICO**") in relation to the Automatic Biometric Recognition System(s).

4. Data Protection

4.1 This Policy shall be read alongside and in addition to the School's Data Protection Policy which applies to all Biometric Data.

4.2 In accordance with the School's Data Protection Policy the School shall process all Biometric Data, in accordance with the key principles set out in GDPR and DPA, namely;

4.2.1 lawfully, fairly and in a transparent manner in relation to the data subject;

4.2.2 by ensuring it is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

4.2.3 by ensuring the processing is adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed;

4.2.4 by ensuring the processing is accurate and where necessary kept up to date with reasonable steps taken to ensure the Personal Data is accurate;

4.2.5 by ensuring it is 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 and

4.2.6 by ensuring it is processed in a manner that ensures the security of Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate or technical measures.

4.3 The School is the Data Controller (as defined by GDPR / DPA) and is responsible for, and be able to demonstrate compliance with clause 4.2.

5. Protection of Freedoms Act 2012

5.1 The School will ensure that the Processing of Biometric Data by an Automated Biometric Recognition System, complies with the additional requirements of

notification and consent set out in sections 26 to 28 Protection of Freedoms Act 2012.

5.2 Before the collection of Biometric Data in relation to any pupil under the age of eighteen (18) the School will:

5.2.1 ensure that each parent of a pupil is notified of the School's intention to use the pupil's Biometric Data as part of an Automated Biometric Recognition System by sending a request for consent substantially in the form of set out in the Guidance as amended from time to time;

5.2.2 use detailed in the School's admissions register, to identify parents;

5.2.3 with due consideration to paragraph 5.3 and 5.4, in the event the School holds information in relation to only one parent, consider whether any reasonable steps can or should be taken to ascertain the details of the other parent;

5.2.4 subject to paragraph 5.4, obtain the written consent of at least one parent before the Biometric Data is taken from the pupil and used i.e.: 'processed'. For the avoidance of doubt in the event a parent objects in writing to the collection / Processing of Biometric Data the School will NOT collect or process Biometric Data for that pupil even where the other parent consents.

5.2.5 In the event the pupil is aged thirteen (13) years or older, and with sufficient understanding, consult the pupil. For the avoidance of doubt Biometric Data will not be collected or processed if the pupil objects either orally or in writing.

5.2.6 provide reasonable alternative means of accessing services for those pupils who will not be using an Automated Biometric Recognition System.

5.3 The School will not need to notify a particular parent or seek his or her consent if the School is satisfied that:

5.3.1 the parent cannot be found, for example, his or her whereabouts or identity is not known;

5.3.2 the parent lacks the mental capacity to object or to consent;

5.3.3 the welfare of the pupil requires that a particular parent is not contacted, for example where a pupil has been separated from an

abusive parent who is not to be informed of the pupil's whereabouts; or

5.3.4 where it is otherwise not reasonably practicable for a particular parent to be notified or for his or her consent to be obtained.

5.4 Where neither of the parents of a pupil can be notified for one reasons set out in paragraph 5.3 (which would mean consent cannot be obtained from either of them), section 27 of the Protection of Freedoms Act 2012 sets out who should, in such circumstances, be notified and who can give consent:

5.4.1 if the pupil is being 'looked after' by a local authority or is accommodated or maintained by a voluntary organisation (i.e. a not-for-profit organisation), the local authority, or as the case may be, the voluntary organisation must be notified and their written consent obtained;

5.4.2 if paragraph 5.4.1 above does not apply, then notification must be sent to all those caring for the pupil and written consent must be gained from at least one carer before the pupil's Biometric Data can be processed (subject to the pupil and none of the carers objecting in writing);

5.5 The School acknowledges that there will never be any circumstances in which the School can lawfully process a pupil's Biometric Data (for the purposes of using an Automated Biometric Recognition System) without one of the persons above having given written consent.

5.5 With due regard to the age and understanding of the pupil, the School will take steps to ensure that pupils understand that they can object or refuse to allow their Biometric Data to be taken/used and that, if they do this, the School will have to provide them with an alternative method of accessing relevant services.

6. Refusal of Consent

6.1 The School will not collect or use Biometric Data for any pupil in the event:

6.1.1 Written notice of objection is received from any parent, notwithstanding consent of another parent; or

6.1.2 Objection verbally or in writing by the pupil.

6.2 Parents and / or pupils' may withdraw consent at any time.

7. Providing alternatives

7.1 Reasonable alternative arrangements must be provided for pupils who do not use Automated Biometric Recognition Systems either because their parents have refused consent (or a parent has objected in writing) or due to the pupil's own refusal to participate in the collection of their biometric data.

7.2 The alternative arrangements should ensure that pupils do not suffer any disadvantage or difficulty in accessing services/premises etc. as a result of their not participating in the Automated Biometric Recognition System. Likewise, such arrangements should not place any additional burden on parents whose children are not participating in such a system.

8. Data protection impact assessments (DPIAs)

8.1 Prior to implementing any system that involves the Processing of Biometric Data the School will carry out a Data Protection Impact Assessment ("**DPIA**").

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

8.3 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; and
- Identify any additional measures to mitigate those risks.

8.4 When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered.

8.5 If a high risk is identified that cannot be mitigated, the DPO will consult the Information Commissioners Office ("**ICO**") before the processing of the Biometric Data begins.

8.6 The ICO will provide the School with a written response (within eight (8) weeks or fourteen (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.

8.7 The School will adhere to any advice from the ICO.

9. Retention of Data

9.1 Biometric Data shall be retained:

9.1.1 Where the Biometric Data forms part of the pupil's educational record, in accordance with the School's Data Protection Policy and / or Data Retention Policy; or

9.1.2 Where the Biometric Data does not form part of the pupil's' educational record for example where it is collected to access school lunch, for the minimum period necessary. For the avoidance of doubt any Biometric Data that does not form part of the pupil's educational record shall be deleted upon the pupil's removal form the School roll for any reason.

9.2 In the event a parent or pupil withdraw consent at any time, any Biometric Data held should be deleted, unless required to be retained in accordance with Data Protection Legislation.