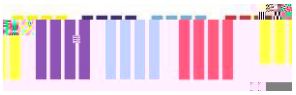
Protection of Biometric Information

Protection of Biometric Information

Contents:

1.	Policy statement	Page 3
2.	About this policy	Page 3
3.	Definition of biometrics data terms	Page 3-4
4.	Roles and responsibilities	Page 4
5.	Data protection principles	Page 5
6.	Data protection impact assessments (DPIAs)	Page 5 -6
7.	Consent	Page 6
8.	Student consent	Page 7 -8
9.	Staff consent	Page 8
10.	Alternative arrangements	Page 8 -9
11.	Data retention	Page 9
12.	Data breaches	Page 9
13.	Subject access requests (SAR)	Page 9
14.	Monitoring and review	Page 9

Appendix 1 [2] Overview of student consent collection Page 10



1

their fingerprints, facial shape, retina and iris patterns, and hand measurements.

3.3 Consent: GDPR requires that consent must be freely given, that the academy must keep a record to demonstrate consent; be able to display prominence and clarity of consent requests; and advise the right to withdraw consent easily and at any time.

3.4 Data controller: Under data protection law, the Trust is the data controller for all biometric information held by the academies.

3.5 Processing biometric information: Processing biometric information 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 student biometric information, e.g. taking measurements from a fingerprint via a fingerprint scanner.
- Storing student biometric information on a database.
- Using student biometric information as part of an electronic process, e.g. by comparing it with biometric information stored on a database to identify or recognise students.

3.6 Special category data: Personal data which the GDPR says is more sensitive, and so needs more protection [2] where biometric information is used for identification purposes, it is considered special category data.

4 Roles and responsibilities

4.1 The Trust Board of Directors are responsible for approving this policy.

4.2 Academy Principals are responsible for ensuring the provisions in this policy are implemented consistently.

4.3 The Trust Data Protection Officer (DPO) is responsible for;

- Monitoring the academy's compliance with data protection legislation in relation to the use of biometric information.
- Advising on when it is necessary to undertake a data protection impact assessment (DPIA) in relation to the academy's biometric system(s).
- Being the first point of contact for the Information Commissioners Office (ICO).

5 Data protection principles

5.1 The academy processes all personal data , including biometric information , in

6.5 If a high risk is identified that cannot be mitigated, the DPO will consult the ICO before the processing of the biometric information begins.

6.6 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 act ion. In some cases, the ICO may advise the school to not carry out the processing.

6.7 The Trust will adhere to any advice from the ICO.

7 Consent

7.1 Prior to any biometric recognition system being put in place or processing of biometric information , the academy must request written consent for the use of biometric information .

7.2 Consent must be freely given. Academies must request written consent advising an explicit yes or no answer to consent ing to the processing of biometric information .

7.3 Consent must not be gained through an opt -out option.

7.4 If there is no reply to the consent request, the academy must determine this as consent is not provided.

7.5 The academy must keep a record of consent as p art of the student /staff file.

7.6 Request for consent from individuals must advise the following:

@Details about the type of biometric information to be taken

@Details of the system(s) that will be used to hold and process the biometric information

@How the biometric information will be used

@The right to refuse or withdraw their consent

@ 7 K H D F D G H P \ · V G X W \ W RP ‡@YU„ Ž¿ • $ ˆt •R„ HrQ NÞ ˆt •XA˜ëñ ˜

8 Student consent

8.1 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 GDPR Instead, the consent requirements for biometric information is imposed by section 26 of the Protection of Freedoms Act 2012.

8.2 In line with both the Protection of Freedoms Act 2012 and GDPR for student V · L Q Year 9 or above, the academy will request consent from the student as well as

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 student and written consent will be obtained from at least one carer before the student's biometric information is processed.

8.9 The academy will not process the biometric information of a student under the age of 18 in the following circumstances:

- The student (verbally or non-verbally) objects or refuses to participate in the processing of their biometric information
- No parent or carer has consented in writing to the processing.
- A parent or carer of the student has objected in writing to such processing, even if another parent has given written consent.

8.10 Parents and students may withdraw consent at any time. Where this happens, any biometric information relating to the student that has already been captured must be deleted.

8.11 If a student objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric information, the academy will ensure that the student's biometric information is not taken or used as part of a biometric recognition system, irrespective of any consent given by the student's parent(s).

8.12 Consent is considered valid for the duration of a student's time at the academy unless consent is withdrawn by the student or parent.

9 Staff consent

9.1 Where staff members use the academy's biometric system(s), their consent will be obtained from them before they use the system.

9.2 Staff and other adults can object to taking part in the academy's biometric system(s) and can withdraw their consent at any time. This must be in writing. Where this happens, any biometric information relating to the individual that has already been captured must be deleted.

9.3 For staff, consent is considered valid for the duration of employment, unless consent is withdrawn.

10 Alternative arrangements

10.1 Parents, students

10.2 Where an individual objects W R W D N L Q J S D U W L Q biometric W K H system(s), reasonable alternative arrangements will be provided that allow the individual to access the relevant service, e.g. where a biometric system uses student · V I L Q J H U S U L Q W V W R S D \ student's fingerprint to access a pre-programmed card, unique number or other suitable means determined by the academy.

10.3 Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service or result in an y additional burden being placed on the individual (and the student · V S D U H Q W V Z K H relevant).