



## COMDA-13-PROTECTION OF BIOMETRIC DATA

### 1 INTRODUCTION

- 1.1 This policy sets out how all biometric data, regardless of origin, will be kept securely, on the Trust's systems.
- 1.2 This ensures compliance with the appropriate legal frameworks:
  - Data Protection Act (2018)
  - General Data Protection Regulations (2018)
  - Protection of Freedoms Act (2012)
  - Human Rights Act (1998)
  - Public Sector Equality Act Duty (2011).
- 1.3 This policy deals with one specific section of Data Protection and must be read in conjunction with the COMDA-03-Data Protection policy.

### 2 ROLE OF TRUST BOARD AND COMMITTEES

- 2.1 The Trust Board has overall responsibility for ensuring compliance with all relevant data protection obligations.

### 3 ROLE OF PRINCIPAL AND SENIOR LEADERSHIP TEAM

- 3.1 The Principal acts as the representative of the Data Controller on a day-to-day basis and must ensure that:
  - The additional risks associated with using automated biometric technology are identified and documented appropriately (Data Protection Impact Assessment),
  - Consult with the Information Commissioners Office (ICO), if necessary, to ensure that the wider duties of the legal frameworks are enabled<sup>1</sup>.
- 3.2 The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable. They will report directly to the Principal and Trust Board on any data protection issues or recommendations. The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO.
- 3.3 The DPO role is shared with SMBC's Information Governance Team.

### 4 DEFINITIONS

- 4.1 The **Subject** this is the person whose biometric data is to be stored and processed. It can be an adult or a child.

---

<sup>1</sup> See page 8 of

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1092507/Biometrics\\_Guidance\\_July\\_2022.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1092507/Biometrics_Guidance_July_2022.pdf)

- 4.2 The **Person with Parental Responsibility (PPR)** is the “parent of the child and any individual who is not a parent of the child but who has parental responsibility for the child”. Usually these are referred to as parents/carers/legal guardians. Practically this is the person(s) who has parental responsibility by birth or adoptive or appointed body. The person that the Trust will notify and seek consent from.<sup>2</sup> If the child is looked after and is subject to a care order in favour of the local authority or the local authority provides accommodation for the child within the definition of section 22(1) of the Children Act (1989), the Trust is not required to notify or seek consent from birth parents.<sup>3</sup>
- 4.3 **Biometric Data (BD)** is personal information produced after specific technical processing. The data that has been processed relates to a physical, psychological, or behavioural characteristic.<sup>4</sup> The processed data is stored and then used against live data for unique identification. Examples of BD include facial image, voice recognition, fingerprint.
- 4.4 **Automated Biometric Recognition Systems (ABRS)** use technology to measure and individual’s physical or behavioural characteristics by using equipment that operates automatically/electronically. ABRS usually store measurements taken from the physical, behavioural characteristics. They do not store an image of the characteristic itself.
- 4.5 **Processing of biometric data** in this situation includes obtaining, recording, or holding the data, or carrying out any operation on the data including, but not limited to, disclosing it, deleting it, organising it, or altering it. This processing takes place when the ABRS:
- Records the Subject’s fingerprint using a biometric scanner, for storage or ID matching,
  - Stores the BD on a digital system,
  - Uses that data as part of an ID matching exercise.

## 5 CONSENT AND PRIVACY

- 5.1 Consent for the processing of BD must be obtained prior to its use in an ABRS. This will take place when:
- A new student is enrolled,
  - A new member of staff starts.
- 5.2 Consent for the processing of BD must be explicit. It is recorded on our Management Information System (MIS) and must be checked before the BD is acquired:
- Each PPR of a child and the Subject themselves must be notified of the Trust’s intention to use an ABRS,
    - PPRs will be encouraged to discuss the use of the ABRS with the child and to support them in making up their own mind about processing,
  - PPRs and Subjects must be given the opportunity to object to the use of the ABRS, initially and at any point thereafter,

---

<sup>2</sup> Protection of Freedoms Act (2012)

<sup>3</sup> See page 10 of

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1092507/Biometrics\\_Guidance\\_July\\_2022.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1092507/Biometrics_Guidance_July_2022.pdf)

<sup>4</sup> See page 7 of

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1092507/Biometrics\\_Guidance\\_July\\_2022.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1092507/Biometrics_Guidance_July_2022.pdf)

- The data can only be processed if the Subject does not object, and, in the case of a child, if:
  - At least one PPR has consented,
  - No PPR has objected. PPR objections must be written<sup>5</sup>.
  - If there is only one PPR on the admissions register the Principal will take reasonable steps to ascertain the details of the other parent in order to determine their opinion, however, this may not be possible/appropriate; the Trust will rely on the exemption in section 27(1)9a) of the Protection of Freedoms Act (2012) under these circumstances.
- A child’s objection or refusal to participate in the use of any ABRS overrides any parental consent to the processing.<sup>6</sup> A child does not have to object in writing.
- The Trust will make it clear that use of an ABRS is not the only option available. An alternative will be provided which must enable equal access to the service for both the Subject and the PPR.

5.3 The use of the ABRS must be included in the Trust’s [Privacy Notices](#) which must explain:

- How the BD is processed and stored,
- The rights available to the Subject in respect of this processing.

## 6 AUTHOR

6.1 The author of this policy is the Data Protection Officer. They should be contacted for any points of clarification or suggested future amendments.

## 7 VERSION CONTROL

|   |                              |
|---|------------------------------|
| <b>Policy Number</b>                      | COMDA-13                     |
| <b>Policy Name</b>                        | Protection of Biometric Data |
| <b>Version Number</b>                     | 01                           |
| <b>Publication Method</b>                 | External                     |
| <b>Approved by</b>                        | Full Trust Board             |
| <b>Date of Approval</b>                   | March 2024                   |
| <b>Key changes since previous version</b> | 1. No changes required       |
| <b>Next Review Date</b>                   | Annual check for amendments  |

<sup>5</sup> See page 14 of

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1092507/Biometrics\\_Guidance\\_July\\_2022.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1092507/Biometrics_Guidance_July_2022.pdf)

<sup>6</sup> Sections 26 and 27 of the Protection of Freedoms Act (2012) have no lower age limit in terms of a child’s right to refuse to participate in sharing their BD.