SESSET

Protection of Biometric Information Policy

Reviewed and approved by Trustees: 13th December 2023

NEXT REVIEW DATE: SUMMER 2024

1. **Protection of Biometrics Policy Statement**

Each school within the SESSET MAT is committed to protecting the personal data of all its students and staff, this includes any biometric data we collect and process. We collect and process biometric data in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected. This policy outlines the procedures the school follows when collecting and processing biometric data.

2. **Biometric information - Legal Framework**

- This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:
- Protection of Freedoms Act 2012
- Data Protection Act 2018
- UK General Data Protection Regulation (GDPR)
- DfE (2018) 'Protection of biometric information of children in schools and colleges'

3. **Definitions**

- **Biometric data:** Personal information about an individual's physical or behavioural characteristics that can be used to identify that person, including their fingerprints, facial shape, retina and iris patterns, and hand measurements.
- **Automated biometric recognition system:** A system 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 to recognise or identify the individual. **Processing biometric data:** Processing biometric data 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 students/staff biometric data, e.g., taking measurements from a fingerprint via a fingerprint scanner.
    - Storing students/staff biometric information on a database.
    - Using students/staff biometric data as part of an electronic process, e.g., by comparing it with biometric information stored on a database to identify or recognise students.
    - **Special category data:** Personal data which data protection legislation says is more sensitive, and so needs more protection – where biometric data is used for identification purposes, it is considered special category data.

4. **Roles and responsibilities**

The **governors** are responsible for:

- Reviewing this policy in line with the school policy review schedule. The **Headteacher** is responsible for:
- Ensuring the provisions in this policy are implemented consistently.

The **Data Protection Lead** in school is responsible for:

- Ensuring a data protection impact assessment (DPIA) has been completed before biometric data is processed.
- Ensuring appropriate consents have been gained and recorded before biometric data is processed.
- Acting as the first point of contact for individuals whose biometric data is processed by the school.

The **Data Protection Officer (DPO)** is responsible for:

- Advising on the data protection impact assessment covering the use of biometric data in school.
- Monitoring the school's compliance with data protection legislation in relation to the use of biometric data

5. **Data Protection Principles**

- SESSET processes all personal data, including biometric data, in accordance with the key principles set out in data protection legislation.
- SESSET ensures biometric data is:
    - Processed lawfully, fairly and in a transparent manner.
    - Only collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
    - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
    - Accurate and, where necessary, kept up-to-date, and that reasonable steps are taken to ensure inaccurate information is rectified or erased.
    - 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.
    - Processed in a manner that ensures appropriate security of the information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- As the data controller, SESSET is responsible for being able to demonstrate its compliance with the provisions outlined above.

6. **Data Protection Impact Assessments (DPIAs)**

- Prior to processing biometric data or implementing a system that involves processing biometric data, a DPIA will be carried out.
- If a biometric system is already in place and there is no DPIA for it then one must be carried out retrospectively to ensure all risks have been identified and appropriately mitigated.

- The Data Protection Lead will carry out the Data Protection Impact Assessment in school and the school DPO will monitor this and provide support as required during this process.

- 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.

- When assessing levels of risk, the likelihood, and the severity of any impact on individuals will be considered.
- If a high risk is identified that cannot be mitigated, the DPO, in consultation with the school, will contact the ICO before the processing of the biometric data begins. 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. The school will adhere to any advice from the ICO.

7. **Providing consent or objecting**

Please note that the obligation to obtain 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 are imposed by section 26 of the Protection of Freedoms Act 2012.

- Where the school uses student and staff biometric data as part of an automated biometric recognition system (e.g. using students' fingerprints to receive school dinners instead of paying with cash), the school will comply with the requirements of the Protection of Freedoms Act 2012.
- Written consent will be sought from at least one parent of the student before the school collects or uses a student's biometric data.
- The name and contact details of the student's parents will be taken from the school's admission register.
- Where the name of only one parent is included on the admissions register, the Headteacher will consider whether any reasonable steps can or should be taken to ascertain the details of the other parent.
- The school does not need to notify a particular parent or seek their consent if it is satisfied that:

  - The parent cannot be found, e.g., their whereabouts or identity is not known.
  - The parent lacks the mental capacity to object or consent.
  - The welfare of the student requires that a particular parent is not contacted, e.g., where a student has been separated from an abusive parent who must not be informed of the student's whereabouts.
  - It is otherwise not reasonably practicable for a particular parent to be notified or for their consent to be obtained.

- Where neither parent of a student can be notified for any of the reasons set out above, consent will be sought from the following individuals or agencies as appropriate:
- If a student is being 'looked after' by the LA or is accommodated or maintained by a voluntary organisation, the LA or 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 data can be processed.
- Notification sent to parents and other appropriate individuals or agencies will include information regarding the following:
  - Details about the type of biometric information to be taken.
  - How the data will be used
  - The parent's and the student's right to refuse or withdraw their consent.
  - The school's duty to provide reasonable alternative arrangements for those students whose information cannot be processed.
- The school will not process the biometric data of a student under the age of 18 in the following circumstances:
  - The student (verbally or in writing) objects or refuses to participate in the processing of their biometric data.
  - No parent or carer has consented in writing to the processing.
  - A parent has objected in writing to such processing, even if another parent has given written consent.
- Parents and students can object to participation in the school's biometric system(s) or withdraw their consent at any time. Where this happens, any biometric data relating to the student that has already been captured will be deleted.
- If a student objects or refuses to participate, or to continue to participate, in activities that involve the processing of their biometric data, the trust will ensure that the student's biometric data is not taken or used as part of a biometric recognition system, irrespective of any consent given by the student's parent(s).
- Where staff members or other adults use the school`s biometric system(s), consent will be obtained from them before they use the system.
- Staff and other adults can object to taking part in the school's biometric system(s) and can withdraw their consent at any time. Where this happens, any biometric data relating to the individual that has already been captured will be deleted.
- Alternative arrangements will be provided to any individual that does not consent to take part in the school's biometric system(s), as outlined in the next section of this policy.

8. **Alternative arrangements**

- Parents, students, staff members and other relevant adults have the right not to take part in the school's biometric system(s).
- Where an individual objects to taking part in the school's biometric 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's fingerprints to pay for school meals, in this scenario, a pin code will be issued as an alternative option, for the student to use.

- Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service or result in any additional burden being placed on the individual (and the student's parents, where relevant).

9. **Data Retention:**

- Biometric data will be managed, retained and disposed of in line with the school's Retention Schedule.
- If an individual (or a student's parent, where relevant) withdraws their consent for their/their child's biometric data to be processed, it will be erased from the school's system. When the child leaves the school or ceases to use the biometric system, their biometric information must be securely erased in line with the school's Retention Schedule.

10. **Monitoring and review:**

The updated policy will be made available to all staff, parents and students on the school website. The Data Protection Lead and Governing Body will review this policy on an annual basis.

11. **Contact**

If you have any questions about this policy, please contact: Data Protection Lead for the School.

12. **Further information and guidance**

This can be found via the following links: Department for Education's 'Protection of Biometric Information of Children in Schools – Advice for proprietors, governing bodies, head teachers, principals and school staff:

https://www.gov.uk/government/publications/protection-of-biometric-informationofchildren-in-schools

ICO guidance on data protection for education establishments:

https://ico.org.uk/fororganisations/in-your-sector/education/

ICO guidance on processing of biometrics:

https://ico.org.uk/for-organisations/guide-todata-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protectionimpact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/