Kirkbie Kendal School Academy Trust

Policy Title:	**Biometric Data (Protection of) Policy**
Policy Reference:	B3
Version:	1.0
Member of Staff Responsible for review:	Business Manager/Network Manager
Governors' Committee/SLT Responsible:	PPM
Status:	Adopted
Date first adopted/accepted by Governing Body:	25 Feb 20
Review Cycle:	2 years
Date of last review:	NEW POLICY
Date for next scheduled review:	Mar 22

Change Record

Version	Date	Description
1.1		
1.2		
1.3		
1.4		

"Kirkbie Kendal School promotes the safeguarding and welfare of children in its care; all policies and procedures support the Child Protection Policy."

PROTECTION OF BIOMETRIC INFORMATION POLICY

1. KIRKBIE KENDAL SCHOOL ACADEMY TRUST PROTECTION OF BIOMETRICS POLICY STATEMENT

Kirkbie Kendal School Academy Trust 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 AND HOW IT SHOULD BE USED

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.
  - General Data Protection Regulation (GDPR).
  - DfE (2018) 'Protection of Biometric Information of Children in Schools and Colleges'.

- This policy operates in conjunction with the following School policies:

  - Data Protection Policy.
  - Records Management Policy.

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 in order 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 student/staff biometric data, e.g. taking measurements from a fingerprint via a fingerprint scanner.
- Storing student/staff biometric information on a database.
- Using student/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 the GDPR 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 Governing Body (PPM Committee) is responsible for:

- Reviewing this policy every two years.

The Headteacher/Business Manager is responsible for:

- Ensuring the provisions in this policy are implemented consistently.

The Data Protection Officer (DPO)/Deputy DPO is responsible for:

- Monitoring the school's compliance with data protection legislation in relation to the use of biometric data.
- Advising on when it is necessary to undertake a Data Protection Impact Assessment (DPIA) in relation to the school's biometric system(s).
- Being the first point of contact for the ICO and for individuals whose data is processed by the school and connected third parties.

5. DATA PROTECTION PRINCIPLES

- The school processes all personal data, including biometric data, in accordance with the key principles set out in the GDPR.

- The school 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, the school 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.

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

- 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 will consult 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 YOUR CONSENT/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 is 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/carer of the student before the School collects or uses a student's biometric data.

- The name and contact details of the student's parent/carers will be taken from the school's admission register.

- Where the name of only one parent/carer 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/carer.

- The school does not need to notify a particular parent/carer or seek their consent if it is satisfied that:

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

- Notification sent to parent/carers 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/carer'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 non-verbally) objects or refuses to participate in the processing of their biometric data.
    - No parent/carer or carer has consented in writing to the processing.
    - A parent/carer has objected in writing to such processing, even if another parent/carer has given written consent.

- Parent/carers 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/carer(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), in line with section 8 of this policy.

8. ALTERNATIVE ARRANGEMENTS

- 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, the student will be able to use ~~cash~~ a pin code for the transaction instead.

- Alternative arrangements will not put the individual at any disadvantage or create difficulty in accessing the relevant service.

9. DATA RETENTION

- Biometric data will be managed and retained in line with the school's Records Management Policy.

- If an individual (or a student's parent/carer, where relevant) withdraws their consent for their/their child's biometric data to be processed, it will be erased from the school's system.

10. MONITORING AND REVIEW

The Governing Body will review this policy every two years. The updated policy will be made available to all staff, parent/carers and students on the school website.

Please note that, when your child leaves the school or ceases to use the biometric system, their biometric information will be securely erased in line with the school's Records Management Policy.

11. 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-information-of-children-in-schools

ICO guidance on data protection for education establishments:

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

12. FREQUENTLY ASKED QUESTIONS

What information should schools provide to parents/carers/students to help them decide whether to object or for parents/carers to give their consent?

Any objection or consent by a parent/carer must be an informed decision – as should any objection on the part of a child. Schools and colleges should take steps to ensure parents/carers receive full information about the processing of their child's biometric data including a description of the kind of system they plan to use, the nature of the data they process, the purpose of the processing and how

the data will be obtained and used. Children should be provided with information in a manner that is appropriate to their age and understanding.

What if one parent disagrees with the other?

Schools and colleges will be required to notify each parent/carer of a child whose biometric information they wish to collect/use. If one parent/carer objects in writing, the school or college will not be permitted to take or use that child's biometric data.

How will the child's right to object work in practice – must they do so in writing?

A child is not required to object in writing. An older child may be more able to say that they object to the processing of their biometric data. A younger child may show reluctance to take part in the physical process of giving the data in other ways. In either case, the school or college will not be permitted to collect or process the data.

Are schools required to ask/tell parents/carers before introducing an automated biometric recognition system?

Schools are not required by law to consult parents/carers before installing an automated biometric recognition system. However, they are required to notify parents/carers and secure consent from at least one parent/carer before biometric data is obtained or used for the purposes of such a system. It is up to schools to consider whether it is appropriate to consult parents/carers and students in advance of introducing such a system.

Do schools need to renew consent every year?

No. The original written consent is valid until such time as it is withdrawn. However, it can be overridden, at any time if another parent/carer or the child objects to the processing (subject to the parent/carer's objection being in writing). When the student leaves the school, their biometric data should be securely removed from the school's biometric recognition system.

Do schools need to notify and obtain consent when the school introduces an additional, different type of automated biometric recognition system?

Yes, consent must be informed consent. If, for example, a school has obtained consent for a fingerprint/fingertip system for catering services and then later introduces a system for accessing library services using iris or retina scanning, then school will have to meet the notification and consent requirements for the new system.

Can consent be withdrawn by a parent/carer?

Parents/carers will be able to withdraw their consent, in writing, at any time. In addition, either parent/carer will be able to object to the processing at any time but they must do so in writing.

When and how can a child object?

A child can object to the processing of their biometric data or refuse to take part at any stage – i.e. before the processing takes place or at any point after his or her biometric data has been obtained

and is being used as part of a biometric recognition system. If a student objects, the school or college must not start to process his or her biometric data or, if they are already doing this, must stop. The child does not have to object in writing.

Will consent given on entry to primary or secondary school be valid until the child leaves that school?

Yes. Consent will be valid until the child leaves the school – subject to any subsequent objection to the processing of the biometric data by the child or a written objection from a parent/carer. If any such objection is made, the biometric data should not be processed and the school or college must, in accordance with the GDPR, remove it from the school's system by secure deletion.

Can the school notify parents and accept consent via email?

Yes – as long as the school is satisfied that the email contact details are accurate and the consent received is genuine.

Will parents/carers be asked for retrospective consent?

No. Any processing that has taken place prior to the provisions in the Protection of Freedoms Act coming into force will not be affected. Any school or college wishing to continue to process biometric data must have already sent the necessary notifications to each parent/carer of a child and obtained the written consent from at least one of them before continuing to use their child's biometric data.

Does the legislation cover other technologies such a palm and iris scanning?

Yes. The legislation covers ***all*** systems that record or use physical or behavioural characteristics for the purpose of identification. This includes systems which use palm, iris or face recognition, as well as fingerprints.

Is parental notification and consent required under the Protection of Freedoms Act 2012 for the use of photographs and CCTV in schools?

No – not unless the use of photographs and CCTV is for the purposes of an automated biometric recognition system. However, schools and colleges must continue to comply with the requirements in the GDPR when using CCTV for general security purposes or when using photographs of students as part of a manual ID system or an automated system that uses barcodes to provide services to students. Depending on the activity concerned, consent may be required under the GDPR before personal data is processed.

The Government believes that the GDPR requirements are sufficient to regulate the use of CCTV and photographs for purposes other than automated biometric recognition systems. Photo ID card systems, where a student's photo is scanned automatically to provide them with services, would come within the obligations on schools and colleges under sections 26 to 28 of the Protection of Freedoms Act 2012, as such systems fall within the definition in that Act of automated biometric recognition systems.

Is parental/carer notification or consent required if a student uses or accesses standard commercial sites or software which use face recognition technology?

The provisions in the Protection of Freedoms Act 2012 only cover processing by or on behalf of a school

or college. If a school or college wishes to use such software for school work or any school business, the requirement to notify parents/carers and to obtain written consent will apply. However, if a student is using this software for their own personal purposes, the provisions do not apply, even if the software is accessed using school or college equipment.

LINKED POLICIES:

- GDPR Policy
- Data Retention Policy
- Freedom of Information Policy