JKHS PROTECTION OF BIOMETRIC INFORMATION IN SCHOOL

This policy has been created in line with the DfE's Protection of Biometric Information of Children in Schools and Colleges guidance, alongside other relevant legislation including Protection of Freedoms Act 2012, Data Protection 2018 and General Data Protection Regulation (GDPR). John Kyrle High School and Sixth Form Centre (JKHS) is committed to protecting the personal data of all its pupils and staff; this includes any biometric data.

1. Definitions

Biometric data is 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. An automated biometric recognition system is where a system 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 enable recognition and identify the individual. Processing of biometric data includes obtaining, recording or holding the data or carrying out an operation on the data included, disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

- Recording pupils' biometric data, e.g. taking measures from a fingerprint via a fingerprint scanner;
- Storing pupils' biometric information on a database; and
- Using pupils' biometric data as part of an electronic process e.g. by comparing it with biometric information stored on a database to identify or recognise pupils.

Biometric data that is used for identification purposes is classed as ***special category data*** which, under GDPR, is deemed sensitive personal data and therefore needs more protection. The school processes all personal data, including biometric data, in accordance with the key principles set out in 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 it is 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 is 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.

2. 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 Data Protection Officer (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 Information Commissioner's Office (ICO) before processing of the biometric data begins. The school will adhere to any advice from the ICO.

3. Notification and consent

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 GDPR, but is imposed by section 26 of the Protection of Freedoms Act 2012. Prior to any processing of a pupil's biometric data, the school will send the pupil's parents an indemnity form for completion and to obtain consent. Written consent will be sought from at least **one parent** of the pupil before the school collects or uses a pupil's biometric data. If staff/adults are also to have biometric data taken, prior consent will be obtained. Where neither parent of a pupil can be notified for any reason with regard to obtaining consent for biometric processing, consent will be sought from the following individuals or agencies, as appropriate:

- If a pupil 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 pupil and written consent will be obtained from at least one carer before the pupil's biometric data can be processed.

The school will not process biometric data of a pupil under the age of 18 if the following applies:

- The pupil (verbally or non-verbally) 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/pupils/other adults including staff can object to participation in the school's biometric system or withdraw their consent at any time. Where this happens, any biometric data relating to the pupil that has already been captured will be deleted.

Alternative arrangements will be provided for any individual that does not consent to take part in the school's biometric system; for the canteen this will be an individual 4-digit PIN that is unique to that pupil/staff member. Any alternative arrangement will not put the individual at any disadvantage or create difficulty in accessing the relevant service.

4. Data retention

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

Policy reviewed:	September 2022
Reviewed by:	Business and Finance Director
Review date:	Summer term 2023
Approved by:	FTB 05.12.2022