



THE PIGGOTT SCHOOL

'...to be a school which inspires and encourages the highest achievement'

PROTECTION OF BIOMETRIC INFORMATION POLICY

Responsibility: Facilities Committee

Review Period: Annually

Approved by the Full Governing Body: 26th February 2020

- 1 Where we use pupils' biometric data as part of an automated biometric recognition system (pupils use finger prints to receive school dinners instead of paying with cash) we will treat the data collected with appropriate care and will comply with the data protection principles as set out in the Data Protection Act 1998 and General Data Protection Regulations (GDPR) and comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.
- 2 *Biometric data* means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.
- 3 An *automated biometric recognition system* uses technology 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.
- 4 We will ensure that each parent of a child is notified of the school's intention to use the child's biometric data as part of an automated biometric recognition system.
- 5 Biometric data is stored on our computer system in a way that is individual to our network and cannot be used to identify pupils/staff to other computer systems or websites.

Consent to process biometric data

- 6 The written consent of at least one parent will be obtained before the data is taken from the child and used (i.e. 'processed'). This applies to all pupils under the age of 18. In no circumstances will a child's biometric data be processed without written consent.
- 7 'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:
 - a. Recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
 - b. Storing pupils' biometric information on a database system; or
 - c. Using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise pupils.
- 8 We do not need to notify a particular parent or seek his or her consent if we are satisfied that:
 - a. the parent cannot be found, for example, his or her whereabouts or identity is not known;
 - b. the parent lacks the mental capacity to object or to consent;
 - c. the welfare of the child requires that a particular parent is not contacted, for example where a child has been separated from an abusive parent who is not to be informed of the child's whereabouts; or
 - d. where it is otherwise not reasonably practicable for a particular parent to be notified or for his or her consent to be obtained.
- 9 Where neither of the parents of a child can be notified for one of the reasons set out above (which would mean consent cannot be obtained from either of them), section 27 of the Protection of Freedoms Act 2012 sets out who should, in such circumstances, be notified and who can give consent:
 - a. if the child is being 'looked after' by a local authority or is accommodated or maintained by a voluntary organisation (i.e. a not-for-profit organisation), the local authority, or as the case may be, the voluntary organisation must be notified and their written consent obtained.
 - b. if paragraph (a) above does not apply, then notification must be sent to all those caring for the child and written consent must be gained from at least one carer before the child's biometric data can be processed (subject to the child and none of the carers objecting in writing).

- 10 We will not process the biometric data of a pupil (under 18 years of age) where:
- a. The child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data; the child does need to object in writing.
 - b. No parent has consented in writing to the processing; or
 - c. A parent has objected in writing to such processing, even if another parent has given written consent.

Withdrawing consent

- 11 The original written consent is valid until such time as it is withdrawn. However, it can be overridden, at any time if another parent or the child objects to the processing (subject to the parent's objection being in writing).
- 12 A pupil's objection or refusal overrides any parental consent to the processing.
- 13 Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.
- 14 When the pupil leaves the school, their biometric data will be securely removed from the school's biometric recognition system.

Alternative means

- 15 Parents and pupils have the right to choose not to use the school's biometric system. We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners via a four digit pin at each transaction if they wish.

Staff members/other adults

- 16 Where staff members or other adults use the school's biometric system, we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.