APPENDIX D – BIOMETRIC DATA

Introduction to Biometric Data

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.

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.

'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. Schools across our Trust who use an **automated biometric recognition system** must comply with the Data Protection Act 2018, UK GDPR and sections 26 to 28 of the Protection of Freedoms Act 2012.

The Ted Wragg Trust treat biometric information of children and its staff as special category data, as such the schools must rely on explicit consent (which satisfies the fair processing conditions for personal and special category data).

Any of our schools in the Ted Wragg Trust, who use a biometric system must follow the practices outlined in the information below.

Data Protection Impact Assessment (DPIA)

Before the introduction of any biometric system, a risk assessment **must** be carried out with a view to evaluating whether the use of biometric data is a necessary and proportionate means of achieving the legitimate objectives set out below. A Data Protection Impact Assessment (DPIA) **must** in all cases be completed and checked with the external DPO service used by our Trust.

The authorised DPIA must be shared with the Compliance Team in the Trust who will maintain a central register for compliance.

Privacy Notices include reference to biometric data.

The Management of Information Policy Suite makes reference to biometric data and these procedures.

Explicit & Informed Consent

As biometric data is special category data, in order to lawfully process this data, there must be a legal basis for processing personal data and a separate condition for processing special category data.

- Schools must ensure that **each** parent/carer of a child is notified of the school's intention to use the biometric data as part of an automated biometric recognition system. In no circumstances can data be processed **without written consent**.
- Explicit written consent must be obtained from a minimum of one parent of **each pupil under the age of 18,** or a carer with parental responsibility, before the data is taken from the child and used. **Sixth-form students** are also covered by this advice.
- Staff must be informed of the intention to introduce the use of biometric data and consent obtained.
- Written consent will be obtained from parents and staff using the relevant consent form, a copy of the template is attached to this Appendix.
- We assume that adults have the capacity to give informed consent unless there is a reason for a concern in this regard. Schools will not need to notify parents if they lack capacity, or have welfare concerns.

- Where a 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 school would not normally be required to notify or seek consent from the birth parents.

❖ Pupil consent

- One parent **must** provide written consent before the biometric system can be used. If **either** parent objects to the processing, data must not be processed. The school will not be permitted to use that child's biometric data and alternatives must be provided.
- The child may also object to the processing of their biometric data. If a child objects, the school **must** not process or continue to process their biometric data, irrespective of whether consent has been provided by the parent(s). **Sixth-form students** are included in this advice.

❖ Withheld or withdrawing pupil consent

Consent can be withheld or withdrawn at any point and in these instances the school will provide reasonable alternative arrangements which will allow the child to access the same facilities that they would have had access to had their biometrics been used.

- Should a parent wish to withdraw their consent, they can do so by writing to the Trust at dataprotection@tedwraggtrust.co.uk requesting that the school no longer use their child's biometric data.
- Pupils who wish for the school to stop using their biometric data do not have to put this in writing but should let Compliance Lead know.

The consent will last for the time period that your child attends the school (unless it is withdrawn).

❖ Consent for staff

The school will seek consent of staff before processing their biometric data.

If the staff member objects, the school will not process or continue to process the biometric data and will provide reasonable alternatives. Staff who wish for the school to stop using their biometric data should do so by writing to the Compliance Lead.

The consent will last for the time period that the staff member remains employed by the School (unless it is withdrawn).

Retention of Biometric Data

Biometric data will be stored by the school for as long as consent is provided (and not withdrawn).

Once a pupil or staff member leaves the school, the biometric data will be deleted from the school's system no later than 72 hours.

Storage of Biometric Data

At the point that consent is withdrawn, the school will take steps to delete their biometric data from the system and no later than 72 hours.

Biometric data will be kept securely and systems will be put in place to prevent any unauthorised or unlawful access/use.

The biometric data is only used for the purposes for which it was obtained and such data will not be unlawfully disclosed to third parties.

Further guidance

Compliance Leads in schools using biometric data must complete the DPO's e-learning module on this area of data protection.

Protection of biometric data of children in schools and colleges
July 2022

[Department for Education non-statutory guidance for the Protection of biometric data of children in schools and colleges (July 2022)]

Process Overview