ODBST Protection of Biometric Data Policy

ODBST Level 1 Statutory Policy:	**ALL** Schools require this policy with **no changes** allowed to core text. No changes are necessary to personalise this with school name and branding, as this is a Trust level policy for use, without change, by all schools. LGBs will **note** adoption in LGB meetings. Review will take place at Trust level, and schools will be notified of updates and review dates as necessary.
Other related ODBST policies and procedures:	**ODBST Data Protection Policy** **ODBST Records Management Policy**
Committee responsible:	**FRAPP**
Approved by:	**FRAPP**
Date Approved:	**24.6.2025**
Review date:	**23.6.2026**

REMOVE/AMEND YELLOW HIGHLIGHT WHERE NOT RELEVANT TO YOUR SCHOOL

1. Statement of intent

The Oxford Diocesan Bucks Schools Trust ('the Trust') is committed to protecting the personal data of all its learners 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 procedure the schools follow when collecting and processing biometric data.

2. Biometric data

2.1. What is 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. At [NAME OF SCHOOL], we use [FINGERPRINT MAPPING **AND/OR** FACIAL RECOGNITION].

All biometric data is considered to be special category data under the UK General Data Protection Regulation (UK GDPR). This means the data is more sensitive and requires additional protection as this type of data could create more significant risks to a person's fundamental rights and freedoms.

Where biometric data is used, the School will carry out a Data Protection Impact Assessment 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.

The result of the Data Protection Impact Assessment will inform the School's use of biometrics and the contents of this policy.

This policy complies with The Protection of Freedoms Act 2012 (sections 26 to 28), the Data Protection Act 2018 and the UK GDPR.

2.2. What is an automatic biometric system

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.

3. The Legal Requirements under UK GDPR

This policy has given due regard to all relevant legislation and guidance including but not limited to:

- Protection of Freedoms Act 2012
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- DfE (2018) 'Protection of biometric information of children in schools and colleges'
- DfE Keeping Children Safe in Education?
- ICO guidance on biometric data and consent

This policy operates in conjunction with the following Trust policies:

- Data Protection Policy
- Records Management Policy

'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.

As biometric data is special category data, in order to lawfully process this data, the School must have a legal basis for processing personal data and a separate condition for processing special category data. When processing biometric data, the School relies on explicit consent (which satisfies the fair processing conditions for personal data and special category data). Consent is obtained using the consent form(s) in the attached appendix. For children under the age of 18 written consent must be received by at least one parent/carer before being able to use their biometric data. Written consent will be sought from any staff member before the school collects their biometric data.

The School process biometric data as an aim to make significant improvements to [DETAILS – for example, cleaning staff attendance, our canteen and lunch facilities or for pupils to sign in/move around the School]. This is to [REASONS for example, ensure efficiency, to do away with the need for swipe cards and cash being used, to safeguard the children].

4. Roles and responsibilities

4.1. The Trust Board is responsible for:

- Reviewing this policy every two years
- Ensuring appropriate governance oversight of biometric data processing across Trust schools

4.2. The Headteacher is responsible for:

- Ensuring the provisions of this policy are implemented consistently
- Ensuring that age-appropriate information about biometric systems and their rights regarding biometric data processing is provided to learners.
- Ensuring that adequate alternative arrangements are in place for all individuals, including staff, who do not consent to biometric processing and whose biometric data will not be used by the Trust.

4.3. The Data Protection Officer (DPO) Judicium is responsible for:

- Monitoring the Trust'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.
- Providing guidance and consent requirements for learners of different ages to the Trust.

4.4. Form Tutors/Class Teachers (as appropriate to school phase) are responsible for:

- Identifying and reporting any concerns about learner consent or objections to biometric processing.

5. Consent and withdrawal of consent

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 UK GDPR. Instead, the consent requirements for biometric information is imposed by section 26 of the Protection of Freedoms Act 2012.

The School will not process biometric information without the relevant consent.

5.1. Consent for pupils

When obtaining consent for pupils, both parents will be notified that the School intends to

use and process their child's biometric information using a biometric data consent form. The School only requires written consent from one parent (in accordance with the Protection of Freedoms Act 2012), provided no parent objects to the processing.

Notification sent to parents/ career will include how the data will be used, the parent's and the child's right to object, refuse or withdraw their consent.

If a parent objects to the processing, then the School will not be permitted to use that child's biometric data and alternatives will be provided [DETAILS OF ALTERNATIVES].

The child may also object to the processing of their biometric data. If a child objects, the School will not process or continue to process their biometric data, irrespective of whether consent has been provided by the parent(s).

Where there is an objection, the School will provide reasonable alternatives which will allow the child to access the same facilities that they would have had access to had their biometrics been used.

Pupils and parents can also object at a later stage to the use of their child's/their biometric data. Should a parent wish to withdraw their consent, they can do so by writing to the School at [insert email address] 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 [NAME] know.

The consent will last for the time period that your child attends the School (unless it is withdrawn). Once consent has been withdrawn or the child has left the school any biometric data will be deleted.

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 learner's parents, where relevant). This is particularly important in secondary schools where peer pressure may be a factor

5.2. Consent for staff

The School will seek consent of staff and other adults before processing their biometric data. If the staff member (or other adult) objects, the School will not process or continue to process the biometric data and will provide reasonable alternatives [DETAILS OF ALTERNATIVES FOR STAFF]. Staff who wish for the School to stop using their biometric data should do so by writing to [NAME].

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

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.

10. Data retention

Biometric data will be managed in line with the Trust's Record Management policy. 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, or consent is withdrawn, the biometric data will be deleted from the School's system no later than 72 hours.

11. 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. These measures are detailed in the Trust's ICT Strategic Plan.

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

12. Breaches

Any breach to the school's biometric system(s) will be dealt with by the Trust DPO (Judicium) in accordance with the Trust's Data Protection Policy and data breach procedures. Any suspected breach involving biometric data will be reported to the Trust DPO immediately and, where required, to the ICO within 72 hours of becoming aware of the breach.

Where a breach involves the biometric data of pupils, parents/carers or the pupils themselves (for those aged 18 and over) will be notified without undue delay where the breach is likely to result in a high risk to their rights and freedoms.

13. The Trust Data Protection Officer

Our Data Protection Officer is Judicium Consulting Limited.
You can contact the DPO using these details:

Address:
5th Floor,
98 Theobalds Road,
London,
WC1X 8WB

Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk

Telephone: 0345 548 7000 (Option 1, then 1)

Appendix 1 – Biometric Consent Form (parent/carer)

Please sign below if you consent to the school taking and using information from your son/daughter's fingerprint as part of an automated biometric recognition system. This biometric information will be used by the school for the purpose of [DETAILS – for example, charging for school meals].

In signing this form, you are authorising the school to use your son/daughter's biometric information for this purpose until he/she either leaves the school or ceases to use the system.

If you wish to withdraw your consent at any time, this must be done so in writing and sent to [DETAILS]. Once your son/daughter ceases to use the biometric recognition system, his/her biometric information will be securely deleted by the school no later than 72 hours.

Please note that pupils can object or refuse to allow their biometric data to be taken/used and if they do this, we will provide them with an alternative method of accessing relevant services. This will be discussed with you or your child (depending on their age and their understanding of their data rights) within school. However, we would encourage you to also discuss this with your child at home to ensure that they are aware of their right to refuse or to change their mind at any time.

For further information on the processing of biometric data, please see our Biometrics Policy which is available [DETAILS - on the school website/in the handbook/from reception].

Parental Consent:

Having ready the above guidance information, I give consent to information from the fingerprint of my son/daughter being taken and used by the school for use as part of an automated biometric recognition system.

I understand that I can withdraw this consent at any time.

Parent/carer name: …….

Signature: ……..

Date: ……

Name of student: ……

Please return a copy of this consent form to [DETAILS].

Appendix 2 – Biometric Consent Form (staff)

Please sign below if you consent to the school taking and using your fingerprint information as part of an automated biometric recognition system. This biometric information will be used by the school for the purpose of [DETAILS – for example to allow them to move freely around the school or for catering].

In signing this form, you are authorising the school to use your biometric information for this purpose until you either leave the school or cease to use the system.

If you wish to withdraw your consent at any time, this must be done so in writing and sent to [DETAILS].

For further information on the processing of biometric data, please see our Biometrics Policy which is available [DETAILS - on the school website/in the handbook/from reception].

Staff Consent:

Having read the above guidance information, I give consent to information from my fingerprint being taken and used by the school for use as part of an automated biometric recognition system.

I understand that I can withdraw this consent at any time.

Staff name: ……

Signature: …….

Date: …….

Please return a copy of this consent form to [DETAILS