

Protection of Biometric Data Policy

The Vyne Community School



Approved at: F&R Committee

Date: 6th October 2026

Last reviewed on: 6th October 2026

Next review due by: October 2027

Contents

1. Policy Statement	Page 2
2. Scope	Page 2
3. Legal and Regulatory Framework	Page 2
4. Definitions	Page 2
5. Governance and Accountability	Page 3
6. Necessity Proportionality and DPIA	Page 3
7. Lawfulness Fairness and Transparency	Page 4
8. Parental Notification and Consent	Page 4
9. The Pupil's Right to Object	Page 4
10. Equivalent Alternatives	Page 5
11. Data Minimisation Purpose Limitation and Accuracy	Page 5
12. Security Suppliers and Disclosure	Page 5
13. Retention and Secure Deletion	Page 5
14. Individual Rights Complaints and Breaches	Page 6
15. Monitoring Review and Assurance	Page 6
Appendix 1: Implementation Checklist	Page 7

1. Policy Statement

The school may use an automated biometric recognition system only where it is necessary and proportionate, a less intrusive method has been considered, the required data protection documentation is in place, and participation is genuinely optional. The school will not obtain or use a pupil's biometric information unless every parent who must be notified has been notified and the required written consent has been received. A pupil's objection always overrides parental consent.

The school currently authorises biometric recognition for cashless catering and recording the provision of lunch. Any additional purpose, including access control, registration or library use, requires a new or revised Data Protection Impact Assessment, privacy information and consent process before it begins.

2. Scope

- This policy applies to biometric information processed by or on behalf of the school in an automated biometric recognition system;
- Sections concerning parental notification and consent apply to pupils under 18. Staff biometric information is governed by data protection and employment law and may be processed only through a genuinely voluntary arrangement; and
- The policy applies to governors, employees, contractors, system suppliers and processors who design, approve, administer, access, host or maintain the system.

3. Legal and Regulatory Framework

- Protection of Freedoms Act 2012, sections 26 to 28;
- UK General Data Protection Regulation;
- Data Protection Act 2018, as amended;
- Department for Education advice, Protection of biometric information of children in schools and colleges;
- Information Commissioner's Office guidance on biometric recognition, special-category data, consent, security and Data Protection Impact Assessments.

The school will keep this policy under review in light of changes to legislation, regulatory guidance and the Data Protection Officer's advice.

4. Definitions

Term	Meaning
Biometric data	Personal data resulting from specific technical processing relating to a person's physical, physiological or behavioural characteristics, which allows or confirms unique identification. Examples include fingerprints, facial features, iris patterns and voice recognition.
Automated biometric	An electronic system that captures or measures a characteristic and automatically compares the resulting biometric information with stored information to recognise or identify a person.

recognition system	
Processing	Any operation involving biometric information, including collecting, recording, creating a template, storing, matching, accessing, disclosing, changing, transferring or deleting it.
Biometric template	A digital representation derived from a biometric characteristic. A template remains biometric personal data even when the original image is not retained.
Parent	A person recognised as a parent for education-law purposes, including a person with parental responsibility. There may be more than one person who must be notified.

5. Governance and Accountability

- The governing body approves this policy and receives assurance that the system is lawful, necessary, proportionate and secure;
- The Headteacher is accountable for implementation and for ensuring that sufficient resources, contracts and controls are in place;
- The Data Protection Officer advises on lawful basis, special-category condition, transparency, consent, the DPIA, processor arrangements, retention, data-subject rights and any breach;
- The system owner administers enrolment, objections, alternatives, access permissions, deletion and supplier liaison and maintains an audit trail;
- Only trained and specifically authorised staff may administer or access the system. Access is reviewed at least annually and promptly removed when no longer required.

6. Necessity Proportionality and DPIA

Before introducing or materially changing biometric processing, the school will complete and obtain Data Protection Officer advice on a Data Protection Impact Assessment. The DPIA will:

- describe the system, the exact purposes, categories of people and data, data flows, supplier access and storage locations;
- demonstrate why biometric recognition is necessary and proportionate and record the non-biometric alternatives considered;
- assess risks to children and adults, including exclusion, coercion, discrimination, false matches, security compromise and the permanence of biometric characteristics;
- identify the Article 6 lawful basis and Article 9 special-category condition and record any additional Data Protection Act 2018 requirement;
- specify security, retention, deletion, audit, incident-response and processor controls; and
- be reviewed before any new purpose, technology, supplier, biometric type or material change is introduced.

The school's Record of Processing Activities, privacy notices and consent materials must be consistent with the approved DPIA. Parental consent required by the Protection of

Freedoms Act does not remove the need for a separate and documented UK GDPR analysis.

7. Lawfulness Fairness and Transparency

- Biometric data used to identify a person uniquely is special-category personal data. The school will document both an Article 6 lawful basis and an Article 9 condition before processing.
- Where the school relies on consent for data protection purposes, it must be freely given, specific, informed, unambiguous and capable of being withdrawn without detriment. Explicit consent must be obtained where Article 9 requires it.
- Because of the imbalance of power in employment, the school will not assume that staff consent is valid. The Data Protection Officer must approve the identified lawful basis and condition. Refusal will not affect employment or access to services.
- Privacy information will describe the controller, Data Protection Officer, purpose, data used, legal basis, recipients, supplier, storage, retention, rights, complaint route and any international transfer or automated decision-making.

8. Parental Notification and Consent

Before taking or using biometric information from a pupil under 18, the school will:

- take reasonable steps to identify and notify each parent, including known non-resident parents;
- provide clear written information about the biometric information, how the system works, each purpose, supplier or recipient, security and retention, the pupil's and parents' rights, and the equivalent alternative;
- obtain written consent from at least one parent before any biometric information is collected or used; and
- record notification, consent, objections, withdrawals and the version of the information supplied.

The school need not notify a particular parent where it is satisfied that the parent cannot be found, lacks capacity, should not be contacted because the child's welfare requires this, or notification is otherwise not reasonably practicable. The reason and evidence must be recorded. If no parent can be notified, the school will follow section 27 of the Protection of Freedoms Act concerning a local authority, voluntary organisation or carers. Biometric information will never be processed without written consent from a person authorised by the Act.

One parent's written objection overrides another parent's consent. A parent may withdraw consent or object later in writing. Processing must stop and the biometric information must be deleted without undue delay, subject only to any strictly necessary evidence of the consent decision itself.

9. The Pupil's Right to Object

- A pupil under 18 may object or refuse at any time. The objection need not be in writing and may be communicated verbally, non-verbally or through refusal to participate.
- A pupil's objection overrides parental consent. Staff must not pressure the pupil, require reasons or treat the pupil less favourably.

- Pupils will receive age-appropriate information explaining the system, their right to refuse or stop, how to do so and the alternative available.
- Any member of staff receiving an objection must notify the system owner promptly. Further biometric use will cease and deletion will be initiated.

10. Equivalent Alternatives

The school must provide a reasonable non-biometric method for any pupil or member of staff who does not participate. Depending on the service, this may include a PIN, card, account lookup or another secure method approved in the DPIA. The alternative will:

- provide equivalent access and not cause delay, embarrassment, stigma, cost or other disadvantage;
- not place an additional burden on a pupil's parents; and
- be explained before consent is sought and remain available immediately following an objection or withdrawal.

11. Data Minimisation Purpose Limitation and Accuracy

- The school will collect only the minimum biometric information needed for the stated purpose.
- The approved biometric information will not be used for a new or incompatible purpose without a fresh DPIA, transparency assessment and, where required, new notification and consent.
- The system will not be used for covert monitoring, behavioural profiling or solely automated decisions producing legal or similarly significant effects unless separately authorised by law and expressly approved following Data Protection Officer advice.
- False matches, failed recognition and accessibility issues will be managed through human review and the non-biometric alternative.

12. Security Suppliers and Disclosure

- Biometric information will be encrypted in transit and at rest, protected by role-based access, strong authentication, logging, patching, backup and tested incident-response controls appropriate to the risk.
- Where the system creates a biometric template, the DPIA and privacy notice will accurately state whether any fingerprint image or other source image is retained. A template will be treated as biometric data.
- A supplier processing data for the school must be appointed under a compliant written data-processing contract, act only on documented instructions, maintain suitable security, assist with rights and breaches, delete or return data when instructed and permit assurance or audit.
- The school will establish where data and backups are stored and will not permit an international transfer unless an approved transfer mechanism and risk assessment are in place.
- Biometric information will not be sold or disclosed for the supplier's own purposes. Disclosure to another body will occur only where lawful, necessary, documented and explained through privacy information unless a lawful exemption applies.

13. Retention and Secure Deletion

Biometric information will be retained only while the person uses the system and consent and the documented legal conditions remain valid. It will be securely deleted without undue delay when:

- a pupil or staff member leaves the school or ceases to use the service;
- a pupil objects or refuses to continue;
- a parent objects in writing or consent is withdrawn;
- staff consent is withdrawn where consent is relied upon;
- the purpose ends, the system is replaced or the information is no longer necessary; or
- the school identifies that the information was collected or used unlawfully.

Deletion will cover live systems, devices and processor-held copies and will address backups in accordance with the approved retention and backup schedule. The school will retain only a minimal administrative record needed to evidence notification, consent, objection, withdrawal and deletion. Completion will be logged and, where appropriate, confirmed to the person or parent.

14. Individual Rights Complaints and Breaches

- Individuals may exercise applicable data protection rights, including access, rectification, erasure, restriction and objection, by contacting the school or Data Protection Officer.
- Concerns should be raised with the Headteacher or Data Protection Officer. Individuals may complain to the Information Commissioner's Office after giving the school an opportunity to respond.
- Any suspected loss, unauthorised access, disclosure or misuse of biometric information must be reported immediately through the school's personal-data breach procedure. The Data Protection Officer will assess containment, risk, notification and lessons learned.

15. Monitoring Review and Assurance

- The system owner will review consent status, objections, users, access rights, deletion records, incidents, supplier assurance and the continuing need for the system at least annually.
- The Data Protection Officer will be consulted on the annual review and any proposed change.
- The governing body will receive proportionate assurance without receiving identifiable biometric information.
- The policy will be republished after material amendment and the notification and consent process repeated where the nature or purpose of processing changes.

Appendix 1: Implementation Checklist

Control	Evidence required	Complete
Purpose and necessity	Approved business case and less intrusive alternatives considered	☐
DPIA	Current DPIA approved after Data Protection Officer advice	☐
Lawful processing	Article 6 basis, Article 9 condition and any DPA 2018 condition recorded	☐
Transparency	Current pupil, parent and staff privacy information	☐
Parents	Each parent identified and notified or a statutory exception recorded	☐
Consent	Written consent received before collection or use	☐
Pupil information	Age-appropriate explanation and objection route in place	☐
Alternative	Equivalent, accessible non-biometric method operating	☐
Supplier	Due diligence and Article 28 processor contract complete	☐
Security	Encryption, access, logging, backups and incident response assured	☐
Retention	Deletion trigger, timescale, backup treatment and audit log defined	☐
Training	Relevant staff trained in objections, alternatives, incidents and deletion	☐
Annual assurance	Access, consent, incidents, supplier and necessity reviewed	☐