

Privacy Notice Addendum: Biometric Data

For use alongside the main Privacy Notices

Purpose of this addendum

This addendum supplements the existing privacy notices used by the school, academy, trust or setting. It explains how biometric data will be approached if a biometric recognition system is used, or proposed for use. It does not replace the existing privacy notices and should be read alongside them.

Biometric data means personal data resulting from specific technical processing relating to a person's physical, physiological or behavioural characteristics. Examples include fingerprints, facial recognition data, iris or retina scans, palm vein data, voice recognition data and similar identifiers. Where biometric data is used for the purpose of uniquely identifying a person, it is special category data.

Who this applies to

This addendum applies where biometric data is processed about pupils or students, parents or carers, staff, volunteers, governors, trustees, committee members, visitors or other individuals who may use or be affected by a biometric recognition system operated by, or on behalf of, the school, academy, trust or setting.

When biometric systems may be used

The school, academy, trust or setting will only use biometric systems where there is a clear, necessary and proportionate reason for doing so. Examples may include cashless catering, library access, access control, attendance systems or similar education management purposes. Before introducing or materially changing any biometric system, the relevant data controller will consider whether a less intrusive alternative can achieve the same purpose.

Legal basis and safeguards

Before using biometric data for identification, the relevant data controller will identify an appropriate lawful basis under Article 6 UK GDPR and a separate condition for processing special category data under Article 9 UK GDPR. In most education biometric recognition contexts, explicit consent is likely to be required.

For pupils and students under 18, the school, academy, trust or setting will also comply with the Protection of Freedoms Act 2012. This means parents or carers will be notified before the child's biometric information is processed, the required written parental consent will be obtained, any written parental objection or withdrawal of consent will be respected, and a pupil's or student's own objection or refusal will also be respected.

Data Protection Impact Assessment

A Data Protection Impact Assessment will be completed before introducing, or materially changing, a biometric recognition system. The assessment will consider the purpose of the system, whether the processing is necessary and proportionate, the risks to individuals, the supplier arrangements, security measures, retention arrangements and the availability of reasonable alternatives.

If a Data Protection Impact Assessment identifies a high risk that cannot be mitigated, the processing will not begin until the appropriate further steps have been taken, including consultation with the Information Commissioner's Office where required.

Consent, refusal and alternatives

- Where consent is used, it must be freely given, specific, informed and capable of being withdrawn.
- For pupils and students under 18, the written consent of at least one parent or carer with parental responsibility is required, unless a statutory exception applies, and no parent or carer has objected or withdrawn consent.
- A pupil or student may refuse or object to the use of their biometric data. Their objection does not need to be in writing and will override parental consent.
- A reasonable non-biometric alternative will be provided so that individuals are not disadvantaged because they do not use the biometric system.
- Where consent is withdrawn, or the individual ceases to use the system, the relevant biometric data will be securely deleted unless there is a lawful reason to retain it.

How biometric data will be handled

Where biometric data is used, separate information will be provided explaining the specific system being used, the type of biometric data collected, the purpose of the processing, who will have access to the data, whether a processor or supplier is involved, how the information will be secured, how long it will be retained and how it will be deleted.

Biometric data will only be used for the purpose explained at the point consent is sought or information is provided. It will not be used for unrelated purposes without further assessment and, where required, fresh consent and updated privacy information.

Live facial recognition

Live facial recognition will not be used in a school, academy, trust or education setting. Live facial recognition is different from a controlled biometric recognition system and involves the real-time and potentially indiscriminate capture of biometric data from people passing within range of a camera. Current DfE guidance states that live facial recognition is not appropriate in school and college settings.

Review

This addendum should be reviewed when the school, academy, trust or setting introduces or changes any biometric system, when supplier arrangements change, or when relevant legislation or national guidance is updated.