Biometrics Policy

A biometric recognition system obtains or records information about a person's physical or behavioural characteristics and compares that information with information which has been previously stored to determine whether the person is recognised by the system. The following rules are necessary to ensure that we comply with data protection law and protect the rights of individuals. They ensure that the risks of data processing are well managed.

This policy sets out the rules all staff, governors, contractors and volunteers **must** follow when collecting and managing biometric information.

Policy rules:

1. We must complete a **Data Protection Impact Assessment** (DPIA) for the use of biometric data.
2. The DPIA must be approved by the **Data Protection Officer** prior to the system being used.
3. We must refer to your use of biometric data in our **privacy notices**, ensuring individuals are clear about their rights in relation to its use
4. We must ensure that all students understand that they can **object** or refuse to allow their biometric data to be taken/used
5. We must **gain consent** in writing from at least one parent. Consent is **not** required from the student, even if they are aged 12 or over (but see point 11)
6. We must **document** that consent has been given
7. We must provide a simple process to **object** and **withdraw consent**
8. We must **document** if consent is withdrawn, or objections are raised
9. We must not continue to hold or use biometric data where consent for its use has been **withdrawn**
10. We must ensure that any Biometric data is securely destroyed when no longer used

11. If any parent/guardian/carer withdraws consent, you must **cease** to hold and use the biometric data even if the other parent/guardian/carer has not withdrawn consent
12. We must accept the view of the **student** if they do not want their biometric data used by the school, regardless of their age. The student's wishes supersede any parent/guardian/carer wishes. If both or either parent has consented and the student does not wish the data to be processed, the student's wishes take precedent.
13. We must ensure that there is an **alternative arrangement** available for any services which use biometrics
14. Ensure that biometric data is held in an encrypted form, and that all available technical and organisational **security** measures are applied
15. The use of biometric data must be recorded in the **records of processing activities (RoPA)** (Framework document H1)
16. We must not share biometric data with 3rd parties unless there is an **appropriate contract** in place protecting the rights of data subjects

How must I comply with these policy rules?

We have related policies, procedures and guidance which tell you how to comply with these rules. These include:

- Data Protection Policy
- Data Handling Security Policy
- Data Breach Policy
- Records Management Policy

- Data Protection Rights Procedure
- Consent Procedure
- Data Breach Procedure
- Subject Access Request Procedure
- Surveillance Procedure
- Retention Schedule

If you are unsure how to comply you must seek advice and guidance from your Data Protection Lead.

What if I need to do something against this policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the SIRO.

References

- Data Protection Act 2018 / UK GDPR
- Article 8, The Human Rights Act 1998
- Protection of Freedoms Act 2012
- ICO Biometric data guidance
- DfE - Protection of biometric information of children in schools and colleges – July 2022

Breach Statement
Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.