

Data Protection & Privacy Policy

Sunbury Education Limited / Sunbury Online Sixth Form College / Maxwell

Document owner	Founder & Director (data-protection accountable owner)
Applies to	All personal-data processing by Sunbury Education Limited, including education delivery, admissions, communications, research/evaluation, websites and Maxwell
Status	Draft for formal adoption
Proposed effective date	15 October 2026
Review cycle	At least annually and after material legal, safeguarding, security or product changes
Next review	October 2027
Approval	To be approved and signed by the Founder & Director before reliance on this policy

1. Purpose

This policy sets out how Sunbury Education Limited (SEL) protects personal data and demonstrates accountability under applicable UK data-protection law. It applies to learners, parents/carers, staff, applicants, school partners, website users and users of Maxwell.

2. Data-protection principles

- Process personal data lawfully, fairly and transparently.
- Collect data for specified, explicit and legitimate purposes.
- Collect only data that is adequate, relevant and limited to what is necessary.
- Keep data accurate and correct it when necessary.
- Retain data only for as long as needed for the stated purpose or legal obligations.
- Protect data with appropriate technical and organisational security.
- Be able to demonstrate compliance and accountability.

3. Children and young people

Where services are likely to be accessed by children, SEL will treat their best interests as a primary consideration and apply age-appropriate privacy protections. Privacy information should be clear and understandable, settings should be protective by default, and collection, profiling and sharing of children's data must be limited to what is necessary and justified.

Before introducing materially new high-risk processing involving children - including significant AI profiling, sensitive-data processing or new school-pilot data flows - SEL will assess privacy risks and complete a Data Protection Impact Assessment (DPIA) where required.

4. Categories of data

Depending on the service, SEL may process limited categories such as:

- identity and contact details; age/date of birth where necessary;
- education, enrolment, attendance, assignment and assessment information;
- account, authentication and security information;
- communications and support records;
- technical usage and audit data;
- accessibility or SEND-related information only where necessary, lawful and appropriately protected;
- safeguarding information only where necessary and subject to stricter access controls.

5. Lawful basis and special-category data

SEL will identify and document an appropriate lawful basis before processing personal data.

Depending on the activity this may include contract, legal obligation, legitimate interests, vital interests, public task where applicable, or consent. Consent will not be used where it is not freely given or where another lawful basis is more appropriate.

Special-category data requires both an Article 6 lawful basis and an additional Article 9 condition where applicable. Criminal-offence data will only be processed where a lawful condition and appropriate safeguards exist.

6. Data minimisation in Maxwell and AI services

- Do not send unnecessary personal or sensitive learner information to AI providers.
- Use pseudonymous or minimised identifiers where practical.
- Prefer provider arrangements that restrict secondary use, model training and unnecessary retention of customer data.
- Separate educational evidence from safeguarding, health or highly sensitive records unless a specific authorised workflow requires access.
- Apply role- and organisation-based access controls so users see only information needed for their authorised task.
- Maintain audit logs for sensitive administrative actions where proportionate.

7. Transparency and rights

SEL will provide appropriate privacy information explaining what data is collected, why, the lawful basis, who it may be shared with, retention, international transfers where relevant, and individual rights. Subject to applicable exemptions, individuals may have rights including access, rectification, erasure, restriction, objection and data portability.

8. Data sharing and processors

Personal data will not be sold. Data may be shared with authorised service providers, schools, awarding/education partners or authorities only where there is a lawful purpose and appropriate safeguards. Processors must be governed by suitable contractual terms. International transfers require an appropriate transfer mechanism and risk assessment where required.

9. Security

- Access is granted on least-privilege and need-to-know principles.
- Authentication, authorisation and school/organisation isolation controls are used where appropriate.
- Sensitive data is protected in transit and at rest using suitable technical controls.
- Secrets and privileged credentials must not be exposed in source code or user-facing systems.
- Security vulnerabilities and incidents are investigated, documented and remediated proportionately.

10. Retention and deletion

SEL will maintain retention rules appropriate to each data category and purpose. Data will be securely deleted or anonymised when no longer needed, subject to legal, contractual, safeguarding, dispute or audit requirements.

11. Personal-data breaches

Suspected personal-data breaches must be reported immediately to the Founder & Director or delegated data-protection owner. SEL will contain and assess the incident, document the decision, and notify the ICO and affected individuals where legally required.

12. Governance and accountability

The Founder & Director is accountable for data-protection governance unless responsibility is formally delegated. New material processing activities must be reviewed for lawful basis, transparency, security, retention and processor arrangements. High-risk child-data processing and material AI changes require documented risk assessment.

References and related documents

ICO - Children's Code / Age Appropriate Design Code: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/>

ICO - Children's Code standards: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/code-standards/>

UK GDPR and Data Protection Act guidance: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/>

Sunbury website: <https://www.sunburycollege.com/>

Approval

Name	Seyed Mostafa Owji
Role	Founder & Director
Signature	
Date	

This policy becomes effective when approved and dated by the authorised signatory.