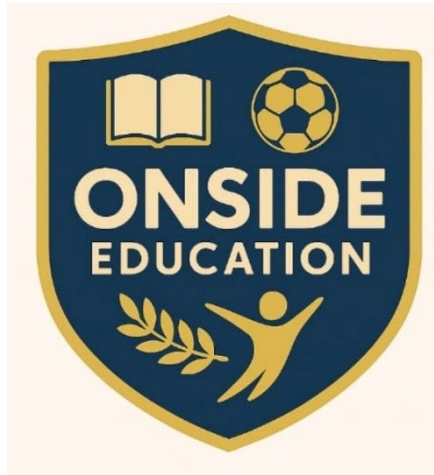




Onside Education Data Protection Policy

Issued date: September 2025

Review Date: September 2026



1. Introduction

Onside Education collects, uses and stores personal data about staff, students, parents/carers, visitors and other individuals in order to operate effectively as an alternative provision provider and to meet its legal obligations.

We recognise our responsibility to handle all personal data:

- Lawfully
- Fairly
- Transparently
- Securely

This policy explains how Onside Education complies with:

- **UK General Data Protection Regulation (UK GDPR)**
- **Data Protection Act 2018**
- Relevant education, safeguarding and employment legislation (including **Keeping Children Safe in Education**).

This policy applies to:

- All staff (permanent, temporary, agency)
- Volunteers
- Contractors and service providers
- Any person acting on behalf of Onside Education

It should be read alongside:

- Online Safety and ICT Acceptable Use Policy
- Safeguarding & Child Protection Policy
- Staff Behaviour / Code of Conduct
- Complaints Policy

This policy is reviewed annually or earlier if there are changes in legislation or guidance.

2. What is Personal Data?

Personal data is any information relating to an identified or identifiable individual.

Examples include (but are not limited to):

- Name, address, email, phone number
- Date of birth, gender
- Assessment and attendance records
- Behaviour, safeguarding and pastoral records
- HR and payroll records
- Photographs and CCTV images
- Online identifiers (e.g. usernames, IP addresses)

Special Category Personal Data

This is personal data that requires additional protection. It includes information about:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Physical or mental health
- Genetic and biometric data (for identification)
- Sexual life or sexual orientation

Onside Education will only process special category data where:

- There is a lawful basis and appropriate condition under UK GDPR / DPA 2018; and
- Appropriate safeguards are in place.

Criminal Convictions Data

Data relating to criminal convictions and offences will only be processed where legally authorised (e.g. safeguarding / DBS checks) and strictly on a need-to-know basis.

3. Data Protection Principles

Onside Education complies with the **seven principles** set out in Article 5 of UK GDPR. Personal data must be:

1. Lawful, fair and transparent

- o Processed lawfully, fairly and in a way that is clear to individuals.

2. Purpose limited

- o Collected for specified, explicit and legitimate purposes and not used for incompatible purposes.

3. Data minimised

- o Adequate, relevant and limited to what is necessary for the stated purposes.

4. Accurate

- o Accurate and, where necessary, kept up to date. Inaccurate data is corrected or erased without delay.

5. Storage limited

- o Kept in an identifiable form for no longer than is necessary for the purposes.

6. Secure (integrity and confidentiality)

- o Processed in a way that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage.

7. Accountability

- o Onside Education is responsible for, and must be able to demonstrate, compliance with all of the above principles.

We demonstrate accountability through:

- Policies and procedures
- Staff training
- Records of processing activities
- Data Protection Impact Assessments (where required)
- Breach logs and audit trails

4. Lawful Bases for Processing

Onside Education processes personal data only where a lawful basis under UK GDPR applies.

The lawful bases most commonly relied upon are:

Public Task

Processing necessary for the provision of education, safeguarding, attendance monitoring, behaviour management, assessment, curriculum delivery, SEND support, examination arrangements and statutory educational functions.

Legal Obligation

Processing required to comply with legal duties, including:

- Independent School Standards
- Safeguarding duties
- KCSIE
- Health and safety legislation
- Equality Act 2010
- Employment legislation
- Tax and payroll requirements

Vital Interests

Processing necessary to protect life or prevent serious harm, particularly in emergencies or safeguarding situations.

Contract

Processing necessary for employment contracts, service agreements and commissioned provision arrangements.

Legitimate Interests

Processing necessary for the effective management of Onside Education where those interests are not overridden by the rights and freedoms of the individual.

Consent

Consent will only be relied upon where appropriate and will not normally be used where another lawful basis applies.

Examples may include:

- Marketing materials
- Certain photographs
- Media publications
- Optional activities

Consent may be withdrawn at any time.

5. Privacy Notices

Onside Education will publish and maintain privacy notices explaining:

- What information is collected
- Why it is collected
- The lawful basis for processing
- Who information may be shared with
- How long information is retained
- Individual rights
- How complaints may be made

Separate privacy notices may be provided for:

- Pupils
- Parents/carers

- Staff
- Volunteers
- Contractors
- Job applicants

Privacy notices will be available on request and via the school website.

Publication of Privacy Notices

Onside Education will publish privacy notices on the school website and make them available to pupils, parents/carers, staff, volunteers, contractors and applicants at the point personal information is collected.

Privacy notices will explain:

- What personal data is collected.
- Why the information is collected and used.
- The lawful basis for processing.
- Who information may be shared with.
- How long information will be retained.
- Individual rights under UK GDPR.
- How concerns or complaints can be raised.

Privacy notices will be reviewed regularly and updated where there are significant changes to processing activities, legislation or guidance.

6. Collection, Use and Sharing of Personal Data

Why Onside Education Processes Personal Data

Pupils and Parents/Carers

Onside Education processes personal data to support the effective delivery of education, safeguarding and pupil welfare. This includes:

- Delivering education, mentoring and alternative provision programmes.
- Monitoring and reporting on attendance, progress, behaviour and wellbeing.
- Providing pastoral, SEMH and SEND support.

- Safeguarding pupils and promoting their welfare.
- Meeting statutory, regulatory and contractual obligations.
- Liaising with commissioning schools, local authorities, health services and other agencies.
- Organising educational visits, work experience, enrichment activities and off-site learning.
- Communicating with parents/carers regarding progress, attendance, behaviour, safeguarding and school events.
- Supporting quality assurance, service development and educational planning.

Staff

Personal data relating to staff is processed to:

- Recruit, appoint and manage employees and volunteers.
- Undertake safer recruitment and safeguarding checks.
- Administer contracts, payroll, pensions and benefits.
- Monitor attendance, performance, training and professional development.
- Support health, wellbeing and workplace safety.
- Manage disciplinary, grievance and capability procedures.
- Fulfil safeguarding and statutory employment obligations.
- Provide employment references and regulatory returns.

Special Category Data

Onside Education may process special category personal data where necessary and lawful to:

- Provide appropriate educational, pastoral, medical or SEND support.
- Implement reasonable adjustments.
- Safeguard pupils and staff.
- Meet equality, employment or safeguarding obligations.

- Fulfil statutory reporting requirements.
- Obtain explicit consent where required.

7. Collection of Personal Data

Personal data may be obtained directly from individuals or from authorised third parties.

Sources include:

- Admission, referral and application forms.
- Employment and HR documentation.
- Contact forms, online portals and school systems.
- Emails, telephone calls, meetings and correspondence.
- Commissioning schools and previous educational settings.
- Local authorities, health professionals and social care services.
- Safeguarding agencies and multi-agency partners.
- DBS and safer recruitment processes.
- CCTV systems, access-control systems and school IT networks.

8. Information Sharing and Safeguarding

Onside Education recognises that effective safeguarding relies upon timely, lawful and proportionate information sharing.

Personal information may be shared without consent where necessary to:

- Safeguard a child or vulnerable individual.
- Protect an individual from harm.
- Prevent or detect crime.
- Fulfil statutory safeguarding duties.
- Support multi-agency working and child protection processes.

Information may be shared with:

- Children's Social Care.
- Police.
- Local Authorities.
- Health Services and CAMHS.
- Youth Justice Services.
- Commissioning Schools.
- Alternative Provision Partners.
- Other statutory safeguarding agencies.

All information sharing will be undertaken in accordance with:

- UK GDPR.
- Data Protection Act 2018.
- Keeping Children Safe in Education (KCSIE).
- Working Together to Safeguard Children.

Data protection legislation is not a barrier to sharing information where there is a lawful basis and a failure to share could place a child or vulnerable person at risk.

9. CCTV, Images and Device Monitoring

Onside Education operates systems that may collect personal data through:

- CCTV systems.
- Access-control systems.
- School-owned devices.
- Network monitoring systems.
- Filtering and monitoring software.
- Online learning platforms.

This information is processed to:

- Safeguard pupils, staff and visitors.
- Protect school property.
- Prevent and detect crime.
- Maintain network security.
- Fulfil safeguarding obligations.

All processing will be proportionate, necessary and undertaken in accordance with UK GDPR and the Data Protection Act 2018.

Further information can be found within the:

- CCTV Policy.
- Online Safety Policy.
- Filtering and Monitoring Procedures.

10. Data Protection Impact Assessments (DPIAs)

Where processing activities are likely to present a high risk to individuals' rights and freedoms, Onside Education will complete a Data Protection Impact Assessment (DPIA).

Examples may include:

- New software platforms.
- Biometric technologies.
- CCTV expansion projects.
- New safeguarding databases.
- Significant information-sharing arrangements.

DPIAs will be reviewed by the Compliance Manager and approved by the Proprietor where appropriate.

The Compliance Manager role is currently undertaken by the Programme Lead unless otherwise designated by the Proprietor.

Records of Processing Activities (ROPA)

In accordance with Article 30 of UK GDPR, Onside Education will maintain Records of Processing Activities (ROPA).

These records will identify:

- Categories of personal data processed.
- Categories of data subjects.
- Purposes of processing.
- Lawful bases relied upon.
- Data sharing arrangements.
- Retention periods.
- Security measures.
- International data transfers where applicable.

The Compliance Manager will maintain and review the ROPA register periodically to ensure ongoing compliance with data protection legislation.

11. International Data Transfers

Where personal data is transferred outside the United Kingdom, Onside Education will ensure that appropriate safeguards are in place to protect individuals' rights and freedoms.

Safeguards may include:

- UK adequacy regulations.
- International Data Transfer Agreements (IDTAs).
- Standard Contractual Clauses.
- Approved certification mechanisms.

Personal data will not be transferred internationally unless an appropriate level of protection can be demonstrated.

Data Retention Schedule

Onside Education maintains a Data Retention Schedule which sets out the retention periods applicable to pupil, safeguarding, personnel, financial, governance and operational records.

Retention periods are determined by:

- Statutory requirements.
- Safeguarding guidance.
- Regulatory expectations.
- Limitation periods for potential claims.
- Operational business needs.

At the end of the relevant retention period, records will be securely destroyed, deleted or anonymised in accordance with the school's information security procedures.

The Data Retention Schedule will be reviewed regularly to ensure compliance with legal and regulatory requirements.

12. Security of Personal Data

Onside Education is committed to protecting personal data against accidental loss, destruction, misuse, unauthorised access, disclosure or alteration.

Appropriate technical and organisational measures will be implemented to safeguard personal information, including:

- Role-based access controls.
- Password protection and multi-factor authentication where appropriate.
- Secure storage of paper records.
- Encryption of devices and systems where necessary.
- Secure backup and recovery procedures.
- Filtering and monitoring systems.
- Cyber-security and data protection training for staff.
- Secure disposal of confidential information.

Staff, volunteers and contractors will only access personal data necessary for the performance of their role and must comply with the school's data protection and information security procedures at all times.

Any actual or suspected data security incident must be reported immediately to the Compliance Manager.

13. Sharing Personal Data

Onside Education will only share personal data where there is a lawful basis to do so and where sharing is necessary, proportionate and appropriate.

Information may be shared with:

- Local Authorities.
- Children's Social Care.
- Police and safeguarding agencies.
- Health services including NHS and CAMHS.
- Commissioning schools and alternative provision partners.
- The Department for Education (DfE).
- Examination boards and awarding organisations.
- Professional advisers, insurers and auditors.
- Approved software, MIS and cloud-service providers.

Where third parties process information on behalf of Onside Education, appropriate contractual arrangements will be in place to ensure compliance with UK GDPR and the Data Protection Act 2018.

Onside Education does not sell personal data and will not share information for commercial marketing purposes without an appropriate lawful basis.

14. Data Retention and Disposal

Onside Education will retain personal data only for as long as necessary to fulfil the purposes for which it was collected and to meet legal, safeguarding, regulatory and operational requirements.

The school maintains a Data Retention Schedule which specifies retention periods for:

- Pupil records.
- Safeguarding records.
- SEND and EHCP records.
- Personnel records.
- Recruitment records.
- Financial records.
- Governance records.
- Health and safety records.

Retention periods are determined by statutory requirements, safeguarding guidance, regulatory expectations and limitation periods for potential legal claims.

When information is no longer required, records will be securely destroyed, deleted or anonymised in accordance with the school's information security procedures.

15. Individual Rights Under UK GDPR

Individuals have rights regarding their personal information under UK GDPR and the Data Protection Act 2018.

These rights include:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure (where applicable).
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights relating to automated decision-making and profiling.

Requests relating to these rights should be submitted to the Compliance Manager.

The school will respond to requests within the timescales required by data protection legislation and will explain any lawful exemptions or restrictions that apply.

16. Subject Access Requests and Data Breaches

Subject Access Requests (SARs)

Any individual, or a parent/carer acting on behalf of a child where appropriate, may request access to personal information held by Onside Education.

Requests should be submitted to the Compliance Manager and will normally be responded to within one calendar month.

Identity and entitlement will be verified before any information is disclosed.

Where appropriate, information relating to third parties will be redacted and statutory exemptions applied.

Personal Data Breaches

A personal data breach is any incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All staff must immediately report actual or suspected breaches to the Compliance Manager.

The Compliance Manager will:

- Assess the nature and severity of the breach.
- Determine whether affected individuals should be informed.
- Determine whether the Information Commissioner's Office (ICO) should be notified.
- Maintain a breach log.
- Implement corrective actions to reduce future risk.

Where required, personal data breaches will be reported to the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

17. Roles, Responsibilities and Complaints

Proprietor

The Proprietor has overall responsibility for ensuring compliance with data protection legislation and information governance requirements.

The Proprietor will receive an annual data protection compliance report which may include:

- Data breaches and near misses.
- Subject Access Requests.
- Data protection complaints.
- Staff training compliance.
- DPIAs completed.
- Information-sharing arrangements.
- Information security risks and actions taken.

Compliance Manager / Data Protection Lead

The Compliance Manager is responsible for:

- Day-to-day data protection compliance.
- Subject Access Requests.
- Data breach management.
- Data Protection Impact Assessments.
- Records of Processing Activities (ROPA).
- Staff training and awareness.
- Information-sharing arrangements.
- Data protection complaints.

Data Protection Complaints

Any individual who believes that Onside Education has not complied with data protection legislation should raise the matter with the Compliance Manager in the first instance.

Email: OnsideAP@u-educate.co.uk

Data protection complaints will be handled in accordance with the school's Complaints Policy and, from June 2026, the relevant Independent School Standards complaints requirements.

Where an individual remains dissatisfied following the school's response, they may refer the matter to the Information Commissioner's Office (ICO).

Website: www.ico.org.uk

Telephone: 0303 123 1113