One Success Privacy Policy

Effective Date: 03/03/2026
Policy Owner: Tahmin Choudhury (Data Protection Officer)
Review Date: Annually or as required

1. Introduction

One Success ("the Organisation") is fully committed to protecting the privacy, confidentiality, and security of personal data. This Privacy Policy outlines how we collect, process, store, and share personal data in compliance with the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018**, and other relevant legislation.

This policy applies to all personal data relating to students, families, staff, partners, volunteers, contractors, and users of our digital platforms, websites, and services.

All staff, volunteers, contractors, and third-party partners who handle personal data must comply with this policy. Non-compliance may result in disciplinary or legal action.

For questions about this policy or how your data is handled, please contact our **Data Protection Officer (DPO)**:

Tahmin Choudhury (DPO)
Email: admin@one-success.co.uk
Phone: 0207 870 6291

---

2. Scope of the Policy

This Privacy Policy applies to **all personal data** processed by One Success, regardless of format (digital, paper, or verbal). It includes data relating to:

- **Students and Prospective Students:** Enrolment, academic progress, communications, and support.
- **Parents and Guardians:** Contact details, emergency information, and household data.
- **Staff and Contractors:** Employment, performance management, and professional development records.
- **Partner Organisations:** Universities, colleges, educational agencies, local authorities, youth organisations, and international partners.
- **Website and Digital Users:** Data collected through online forms, cookies, subscriptions, and digital engagement.

Processing activities include the collection, recording, storage, sharing, use, retention, and secure disposal of personal data.

---

3. Roles and Responsibilities

3.1 Data Protection Officer (DPO)

The DPO oversees data protection compliance and is responsible for:

- Monitoring adherence to UK GDPR and the Data Protection Act 2018
- Responding to Data Subject Access Requests (DSARs) and other individual rights requests

- Advising on lawful bases for processing and conducting Data Protection Impact Assessments (DPIAs)
- Investigating and reporting personal data breaches
- Maintaining records of processing activities

3.2 Senior Management

Senior Management is accountable for compliance and is responsible for:

- Allocating resources to support data protection
- Promoting a culture of accountability
- Approving policies and corrective actions
- Considering data protection risks strategically

3.3 Staff, Volunteers, and Contractors

All personnel handling personal data must:

- Process data lawfully, fairly, and transparently
- Access data only for legitimate purposes
- Maintain confidentiality and security
- Complete mandatory GDPR training
- Report data breaches promptly

3.4 Partners and External Organisations

Third-party processors must:

- Comply with GDPR and contractual safeguards
- Only process data for agreed purposes
- Implement appropriate technical and organisational measures
- Notify the Organisation of any breaches

---

4. Data Protection Principles

One Success adheres to **UK GDPR principles**:

1. **Lawfulness, Fairness, and Transparency:** Individuals are informed of how their data is used, and processing is fair and lawful.
2. **Purpose Limitation:** Data is collected for specific, legitimate purposes only.
3. **Data Minimisation:** Only necessary data is collected and processed.
4. **Accuracy:** Data is kept up to date; inaccuracies are corrected or erased.
5. **Storage Limitation:** Data is retained only as long as necessary, then securely disposed of.

6. **Integrity and Confidentiality:** Technical and organisational measures protect data from unauthorised access or loss.
7. **Accountability:** One Success documents and demonstrates GDPR compliance at all times.

---

5. Categories of Personal Data

We may process:

- **Student Data:** Academic history, grades, references, personal statements, SEND information, digital accounts
- **Family/Guardian Data:** Contact info, emergency contacts, socio-economic information
- **Application Data:** UCAS applications, CVs, supporting documents, scholarships
- **Visa and Immigration Data:** Passport, visa, residency permits, CAS documents
- **Financial Data:** Payments, invoices, bank details, scholarship disbursements
- **Digital Data:** IP addresses, browser/device info, cookies, website usage
- **Special Category Data:** Health, disability, ethnicity, religious beliefs (processed only with consent or legal justification)
- **Children's Data:** Collected with enhanced protections, parental/guardian consent, and age-appropriate privacy notices

Data is regularly reviewed for relevance, necessity, and compliance with retention schedules.

---

6. Purposes of Processing

Personal data is processed for:

- **Educational Services:** Applications, mentoring, academic guidance, scholarship support, visa advice
- **Communication:** Responding to enquiries, sending updates, newsletters, and event invitations
- **Safeguarding and Legal Compliance:** Child protection, regulatory obligations, immigration compliance
- **Monitoring & Evaluation:** Student progress, program performance, internal audits
- **Marketing & Outreach:** Promotional activities with consent
- **Research & Service Improvement:** Analysing anonymised data for quality enhancement
- **Partnership Operations:** Sharing necessary data with trusted partners

Data is never used for purposes incompatible with its original collection.

---

7. Lawful Basis for Processing

Processing is based on:

- **Consent:** Clear, informed consent for marketing, testimonials, or special category data
- **Contractual Necessity:** Required for delivering educational services and fulfilling agreements
- **Legal Obligation:** Compliance with laws, safeguarding, financial, and regulatory requirements
- **Legitimate Interests:** Service development, administration, security, and student support

Special category data requires additional Article 9 legal conditions.

---

8. Data Sharing

Data may be shared with:

- Universities, colleges, and scholarship providers
- Education agencies and international partners
- Local authorities and youth organisations
- Legal, immigration, or professional advisers

All sharing is limited to the minimum necessary, under GDPR-compliant contracts, and with explicit consent where required. Data is never sold or shared for unrelated commercial purposes.

---

9. Data Retention

Personal data is retained only as long as necessary:

Data Type	Retention Period
Student applications & academic records	7 years after study completion
Financial records	7 years (tax compliance)
Partnership agreements	7 years or as per contract
Marketing data	Until consent withdrawn
Safeguarding records	Statutory minimum retention

Data is securely deleted, destroyed, or anonymised after retention. Exceptions apply only for legal claims, investigations, or safeguarding needs.

---

10. Data Security

We implement robust security measures:

- **Digital Security:** Encrypted storage, secure cloud services, 2FA, vulnerability testing

- **Access Control:** Role-based permissions, least privilege principle, regular reviews
- **Physical Security:** Locked storage, restricted access, shredding of paper records
- **Staff Training:** GDPR, safeguarding, and secure handling procedures
- **Breach Response:** Prompt reporting, containment, ICO notification, and corrective action

---

11. Data Subject Rights

You have the right to:

1. Access your data
2. Rectify inaccuracies
3. Erase data (Right to be Forgotten)
4. Restrict or object to processing
5. Data portability
6. Withdraw consent at any time
7. Lodge a complaint with the **ICO** (ico.org.uk)

Requests should be submitted to the DPO. Response time is typically **one month**, or up to **three months for complex requests**.

---

12. Cookies & Digital Tracking

We use cookies for analytics, performance, engagement, and functionality.

- **Consent:** Non-essential cookies require explicit consent
- **Management:** Users can withdraw consent via browser settings or cookie preference centre
- **Third-Party Cookies:** Subject to their privacy policies and GDPR agreements
- **Retention:** Data is stored only as long as necessary

---

13. Staff Responsibilities

Staff, volunteers, and contractors must:

- Comply with GDPR and this policy
- Report breaches immediately
- Maintain confidentiality and secure handling
- Complete mandatory training
- Cooperate with audits and corrective actions

14. Accountability and Auditing

One Success maintains compliance through:

- Records of Processing Activities (ROPA)
- Regular internal audits and monitoring
- Policy reviews at least annually or after legislative/operational changes
- Documentation of compliance for internal and ICO review
- Monitoring partner adherence through audits and contractual safeguards

---

15. Policy Review

This policy is reviewed annually or when triggered by:

- Legislative or regulatory changes
- Operational changes or new systems
- Data breaches or audit findings

Last Review: 03/03/2026
Next Scheduled Review: 03/03/2027

Data Protection Officer (DPO): Tahmin Choudhury
Email: admin@one-success.co.uk
Phone: 0207 870 6291