NUDGE
EDUCATION

Nudge Education Information Security & Data Protection Policy
(*Incorporating General Data Protection Regulation May 2018)*

September 2025

Review Date; September 2026

Scope of the Policy

This policy applies to all personal data processed by Nudge Education, including that of students, parents and guardians, employees, associates, contractors, commissioners, and website users. It is designed to ensure that our data handling practices comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data Use and Access Act 2025 (DUAA).

It also ensures compliance with the Privacy and Electronic Communications Regulations (PECR) in respect of cookies and online tracking, and it reflects current guidance from the Information Commissioner's Office (ICO). As ICO guidance is under review to reflect DUAA, we note that this policy will be revisited during 2026 to incorporate any further developments.

This policy should be read alongside related documents including our Privacy Notices (for commissioners and students, staff and contractors, and web users), our Confidentiality Policy, Safeguarding Policy, IT and Communications Policy, and our Business Continuity and Breach Management Plan.

Statement of Intent

Nudge Education exists to support some of the most vulnerable young people in the United Kingdom back into education, training, or employment. To deliver this mission, we must process large amounts of personal and sensitive information. We take this responsibility extremely seriously, recognising that the protection of an individual's privacy is central to safeguarding their rights and maintaining their trust in our service.

We are committed to processing all personal data lawfully, fairly and transparently; for specified and legitimate purposes; in a way that is limited to what is necessary; kept accurate and up to date; retained only for as long as necessary; secured against unauthorised or unlawful access, loss, destruction, or damage; and accountable to both individuals and regulators for our decisions.

We also recognise new duties introduced under DUAA, including the obligation to apply the "data protection test" when transferring personal data internationally, the introduction of a new lawful basis of "recognised legitimate interest" for safeguarding and public interest purposes, and the updated right for individuals to raise complaints directly with organisations as well as the ICO.

Roles and Responsibilities

Nudge Education has formally appointed **Data Protection People, The Tannery, Leeds**, as its **Data Protection Officer (DPO)**. The DPO provides independent oversight, advises on obligations, monitors compliance, and acts as our point of contact with the ICO.

The **Data Protection Lead (Operations)** is Brian Mair, who ensures operational compliance across the organisation and acts as the first point of contact for privacy queries at privacy@nudgeeducation.co.uk.

The **Managing Director and Senior Leadership Team** hold ultimate accountability for data protection compliance, while all staff, associates, and contractors must follow this policy and undertake regular training.

Collection of Personal Data

We collect data directly from students, parents, employees, contractors, and web users, as well as from commissioners and referrers such as local authorities, schools, education providers, and health or social care professionals. We may also collect limited information from publicly available sources such as LinkedIn in respect of contractors and support professionals.

Where personal data is obtained indirectly, Nudge Education provides privacy information to the individual within one month or at first contact, unless the law provides an exemption.

Types of Personal Data We Process

The personal data that Nudge Education processes depends on the relationship with the individual (student, parent/guardian, commissioner, staff member, contractor, or website user). We apply the principle of data minimisation: collecting only what is necessary for the purpose and retaining it only as long as needed. Categories include:

1. Identity and Contact Information
This includes names, initials, date of birth, gender, addresses, email addresses, telephone numbers, emergency contact details, and where applicable, professional roles or job titles (for commissioners and support professionals).

2. Programme and Education Information
This covers referral details from commissioners, education history, assessments, learning plans, progress notes, safeguarding records, incident reports, case outcomes, and other documentation generated as part of the student's programme. It may also include feedback from students and parents/guardians, or evaluations provided to commissioning authorities.

3. Support Network Information
We hold details about family members, carers, and others involved in the student's support, as well as professionals in education, health, social care, youth services, or other agencies. This enables us to coordinate and deliver effective interventions.

4. Special Category Data
In order to safeguard and deliver tailored educational support, we may process data revealing:

- Health conditions (physical and mental health, diagnoses, treatment or support needs).
- Special Educational Needs and Disabilities (SEND).
- Mental health needs, including behavioural or psychological assessments.
- Ethnicity or religion, where relevant to ensuring cultural or religious needs are respected in the programme.

This processing is limited to what is strictly necessary and is carried out under UK GDPR Article 9 and DPA 2018 Schedule 1 conditions (substantial public interest, health/social care, or vital interests).

5. Criminal Offence Data
In limited cases, we process data about criminal convictions or offences, such as youth offending, anti-social behaviour history, or police involvement. This is only done where necessary for safeguarding, risk assessment, or statutory purposes, and always with additional safeguards. We maintain an **Appropriate Policy Document (APD)** to support this processing in line with the Data Protection Act 2018.

6. Business, Employment and Financial Records
We process personal data relating to employees, associates, and contractors (including applications, contracts, training records, payroll, and performance information). We also process information about commissioners and partner organisations, including contact details, financial transactions, invoices, and correspondence.

7. Website and Digital Information
For users of our website and digital platforms, we collect:

- Contact details provided via forms (e.g., name, email, phone number).
- Technical and usage data such as IP addresses, device identifiers, browser type, operating system, and pages visited.
- Cookie and analytics data, used for improving website performance and user experience. Strictly necessary cookies are set automatically, while analytics and marketing cookies require consent under PECR. We respect Do Not Track and Global Privacy Control (GPC) signals where technically feasible.

8. Images and Testimonials
Where consent has been given, we may use photographs, video recordings, or written testimonials for publicity, marketing, or case studies. Consent can be withdrawn at any time.

Lawful Bases for Processing

We rely on several lawful bases for processing under UK GDPR and DUAA:

- **Legitimate interests** (Article 6(1)(f)): for delivering core educational support programmes and monitoring outcomes, in the interests of students and commissioners. We do not rely on contract with parents or students for this

processing.

- **Legal obligations** (Article 6(1)(c)): e.g., employment law, safeguarding duties, and regulatory reporting.

- **Public task** (Article 6(1)(e)): where acting on behalf of a commissioning public authority.

- **Consent** (Article 6(1)(a)): for activities such as publicity images, testimonials, or non-essential cookies. Explicit consent (Article 9(2)(a)) is required where special category data is involved.

- **Recognised legitimate interest** (DUAA): for certain safeguarding and public interest processing, particularly where balancing tests are not required.

For **special category data**, we rely on:

- Article 9(2)(g) substantial public interest (safeguarding children and vulnerable individuals),

- Article 9(2)(h) health or social care,

- Article 9(2)(c) vital interests in emergencies.

For **criminal offence data**, we rely on DPA 2018 Schedule 1 conditions, supported by our Appropriate Policy Document.

Data Sharing and International Transfers

Personal data may be shared with commissioners, practitioners, contractors, specialist providers, and relevant authorities (e.g., police, NHS, social services) where lawful and necessary. All contractors are bound by confidentiality agreements and Article 28-compliant contracts.

Where data is transferred outside the UK, we use adequacy decisions where available, or the UK International Data Transfer Agreement (IDTA) or UK Addendum to EU Standard Contractual Clauses, supported by supplementary measures where necessary. Under DUAA, we apply the “data protection test” to ensure transfers provide appropriate protection.

Retention of Data

We keep personal data only for as long as necessary:

- **Programme records**: typically six years after the programme ends, or longer if safeguarding or legal claims require.
- **Referrals that do not proceed**: deleted within 28 days.
- **Business records and website enquiries**: retained for up to seven years or until removal is requested.
- **Financial records**: retained for at least six years to meet legal obligations.

At the end of retention periods, data is securely deleted or anonymised.

Children's Information and Consent

For students under the age of 13, we seek consent from a person with parental responsibility where consent is required (e.g., publicity images). For safeguarding and other substantial public interest processing, we rely on lawful bases other than consent, while ensuring transparency.

Security

Nudge Education recognises that safeguarding the confidentiality, integrity and availability of the personal data we hold is fundamental to our work. We therefore implement a layered approach to information security, applying both technical and organisational measures proportionate to the sensitivity of the data and the risks we manage.

We use **encryption** to protect data both in transit and at rest wherever systems support it. This includes secure connections (TLS/SSL) for email and web services, and encryption of storage on laptops, mobile devices and cloud platforms. Where encryption is not technically possible, alternative compensating controls such as restricted access, pseudonymisation or anonymisation are applied.

All devices used to process organisational data are subject to **centralised management**. This allows us to enforce security settings, apply software updates, enable remote wipe in case of loss or theft, and block the installation of unauthorised applications. Access to systems requires **multi-factor**

authentication (MFA), adding a further layer of protection against account compromise.

We apply a principle of **least privilege** when granting access to personal data. Only those staff, contractors or associates who require data to perform their duties are granted access, and this is restricted to the minimum level necessary. Access rights are reviewed regularly, and immediately revoked when an individual leaves the organisation or no longer requires access.

Before engaging third-party service providers who process data on our behalf, we undertake **supplier due diligence**. This includes checking security certifications, assessing technical and organisational safeguards, and ensuring that data protection terms are embedded in contracts in line with Article 28 UK GDPR. Sub-processors are not permitted to access data without our written approval.

Security is not purely technical, and so we invest in **regular staff training and awareness**. All staff, contractors and associates must complete data protection and information security training at induction, with mandatory refresher training every two years or sooner if legal or policy changes require. Targeted training is provided for those in high-risk roles such as safeguarding or IT.

Finally, we maintain a documented **incident management and breach response plan**. This sets out how suspected or actual data breaches are reported, investigated, contained, and, where necessary, reported to the ICO within 72 hours. The plan also covers communication with affected individuals where there is a high risk to their rights or freedoms. Lessons learned from any incidents are used to strengthen controls and reduce the likelihood of recurrence.

We regularly test and review our technical measures, including through system audits, penetration testing where appropriate, and regular reviews of our suppliers and cloud services. Security controls are continuously adapted in response to evolving risks, industry good practice, and ICO guidance.

We also recognise that while internet transmission carries inherent risks, we apply Article 32 security standards to minimise these.

Cookies and Online Tracking

In compliance with PECR and UK GDPR, Nudge Education operates a cookie management system on its website. Strictly necessary cookies run without consent. All analytics, marketing, and social media cookies are set only with explicit consent collected through a cookie banner.

We respect Global Privacy Control (GPC) and Do Not Track signals where technically feasible, treating them as opt-outs from non-essential cookies. Users can withdraw or change cookie preferences at any time.

Data Breach Management

All staff and contractors must immediately report suspected or actual data breaches to the Data Protection Lead. The DPO will assess the risk to individuals, document the breach, and determine whether notification to the ICO is required within 72 hours. Where there is a high risk to individuals, they will be notified promptly.

All breaches, regardless of severity, are logged, investigated, and reviewed to strengthen our controls.

Rights of Individuals

We uphold the rights of individuals to access their data, request rectification or erasure, restrict or object to processing, request data portability, and withdraw consent where it is the lawful basis.

We aim to respond to rights requests within one month, extendable by two months if complex. Some rights may be limited where safeguarding, confidentiality, or legal obligations apply.

Individuals also have the right to raise complaints directly with Nudge Education (privacy@nudgeeducation.co.uk) and to the ICO. We encourage complaints to be raised with us first so we can resolve them.

Training and Awareness

All staff, associates, and contractors receive mandatory training on data protection and information security. Training is refreshed every two years, or sooner when required by legal or policy changes. Updates on breach management, PECR compliance, and DUAA changes are integrated into training programmes.

Monitoring and Review

We maintain a comprehensive Record of Processing Activities (RoPA) that documents all purposes, categories of data, recipients, retention periods, and safeguards. This is regularly reviewed and updated.

This policy is reviewed annually, or sooner if legislation, ICO guidance, or organisational practices change.

References

- UK GDPR and Data Protection Act 2018
- Data Use and Access Act 2025
- ICO Guidance (as of October 2025)
- Privacy and Electronic Communications Regulations (PECR)

Version Number/Date of Update	Author	Date for review
September 2024	Brian Mair	September 2025
September 2025	Brian Mair	September 2026