Data Protection & GDPR Policy

Company: Navigate Education Limited
Issue date: 14/1/2026
Review date: 14/1/2027
Contact: gareth@letusnavigate.com

This policy forms part of Navigate Education Limited's governance and due diligence documentation for partners, schools, and local authorities.

1. Purpose
Navigate Education Limited ("Navigate") is committed to protecting personal data and complying with the UK General Data Protection Regulation (UK GDPR), the EU General Data Protection Regulation (EU GDPR) where applicable, and other relevant international data protection requirements. This policy explains how we handle personal data in a lawful, fair, and transparent way and is designed to support public sector and local authority due diligence and procurement processes.

2. Scope
This policy applies to all personal data processed by Navigate in connection with our services, operations, and relationships with schools, local authorities, partners, and individuals.

3. Definitions
• Personal data: information relating to an identified or identifiable individual.
• Processing: any operation performed on personal data (collection, storage, use, disclosure, deletion).
• Data subject: the individual whose personal data is processed.
• Controller/Processor: in many engagements, schools or local authorities will act as the controller and Navigate will act as a processor for limited administrative processing (for example, invoicing contacts).
Where Navigate determines purposes and means of processing for its own systems (for example, business contacts in our CRM), we act as a controller for that processing.

4. Data protection principles
Navigate processes personal data in line with the core principles of data protection:
• Lawfulness, fairness and transparency
• Purpose limitation
• Data minimisation
• Accuracy
• Storage limitation
• Integrity and confidentiality (security)
• Accountability

5. What personal data we process
Navigate processes a minimal amount of personal data, primarily relating to adult professionals. This includes:
• Professional contact details, typically email addresses (e.g. school staff, local authority staff, partners, clients)
• Organisational and billing information supplied by schools or local authorities for invoicing (e.g. organisation name, billing address, purchase order details, finance contact email)

Navigate does not require, request, or process identifiable personal data about children or young people in order to deliver training and learning services. Where child-related examples or scenarios arise in discussion, we expect these to be anonymised; if any identifiers are used they should be limited to initials only.

6. Lawful bases for processing

We process personal data only where we have a lawful basis, including:

• Contract: where processing is necessary to deliver agreed services or to administer contracts.
• Legal obligation: where processing is required for legal or regulatory compliance (e.g. financial record keeping).
• Legitimate interests: for professional communications and relationship management with organisations and stakeholders, where these interests are not overridden by individuals' rights.

We do not generally rely on consent as our primary lawful basis in our business-to-business and public sector work.

7. How we use personal data

We use personal data to:

• Communicate with schools, local authorities, and partners
• Provide access to training and learning provision via third-party platforms
• Administer contracts, purchase orders, and invoices
• Maintain necessary business records and audit trails
• Improve our services and operational effectiveness (without profiling children or using identifiable child data)

8. Systems, processors, and data sharing

Navigate uses reputable third-party services to operate efficiently and securely.
The main systems used are:

• HubSpot (CRM): used to store professional contact details (e.g. email addresses) and manage professional communications.
• Thinkific (learning platform): used to deliver online learning. Users create their own login credentials. Navigate does not have access to users' passwords and does not view or store password data. We can generate password reset links through the platform where needed.

We share personal data only where necessary and proportionate, and we ensure appropriate contractual protections (including data processing terms) are in place with relevant third-party providers.

9. International transfers

Navigate operates in the UK, EU, and internationally. Where personal data is transferred outside the UK or European Economic Area (EEA), we ensure appropriate safeguards are in place, such as adequacy decisions or standard contractual clauses and/or other lawful transfer mechanisms appropriate to the circumstances.

10. Security of personal data

Navigate takes appropriate technical and organisational measures to protect personal data, including:

• Using reputable cloud platforms with access controls
• Limiting access to authorised personnel
• Applying data minimisation and limiting downloads/export where possible
• Promoting staff awareness and good security practices
• Having a clear incident and breach reporting route

11. Data retention
Navigate retains personal data only for as long as necessary:
• Professional contact details are retained while there is an active working relationship and for a reasonable period afterwards where needed for continuity and record keeping.
• Invoicing and financial records are retained in line with statutory and audit requirements.
Retention is reviewed periodically to ensure we do not keep data longer than needed.

12. Individual rights
Individuals have rights under data protection law, including the right to access their personal data, request correction of inaccurate data, request deletion in certain circumstances, restrict or object to processing, and lodge a complaint with the Information Commissioner's Office (ICO) in the UK or the relevant supervisory authority in the EEA.
Requests can be made using the contact details below. We aim to respond within statutory timescales.

13. Data breaches
Any actual or suspected personal data breach must be reported promptly to Navigate. Where required, we will report qualifying breaches to the ICO within 72 hours and communicate with affected individuals as appropriate.

14. Responsibilities
• Company leadership is responsible for ensuring appropriate governance and compliance.
• All staff, contractors, and associates must handle personal data in line with this policy and report concerns promptly.

15. Review
This policy is reviewed at least annually and updated when necessary to reflect changes in legislation, guidance, or organisational practice.

16. Contact
For data protection enquiries: gareth@letusnavigate.com