Information Security 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 information and systems from unauthorised access, loss, misuse, or disruption. This policy sets out the measures we take to maintain confidentiality, integrity, and availability of information.

This policy supports our Data Protection & GDPR Policy and is designed to meet common public sector and local authority due diligence expectations.

2. Scope:
This policy applies to:
• All employees, contractors, and associates of Navigate
• All information handled by Navigate, whether digital or physical
• All devices and systems used to access Navigate information

3. Information security principles:
Navigate's information security approach is based on:

- **Confidentiality:** information is accessible only to authorised individuals
- **Integrity:** information is accurate and protected from unauthorised alteration
- **Availability:** information and services are available when needed for legitimate business purposes

4. Systems and platforms:
Navigate uses reputable, secure, cloud-based platforms to deliver services and manage information. Key systems include:
• HubSpot (CRM)
• Thinkific (online learning platform)
We choose platforms with appropriate security controls and contractual protections.

5. Access control and authentication:
• Access is restricted to authorised individuals and provided on a role-appropriate basis
• Credentials must not be shared
• Access is reviewed when roles change or individuals leave
Navigate does not have access to user passwords for the online learning platform.

6. Secure working practices:
Staff and associates are expected to:
• Keep devices secure (e.g. screen locks, secure storage)
• Use strong, unique passwords and (where available) multi-factor authentication
• Avoid using unsecured public Wi■Fi for sensitive work unless using appropriate safeguards
• Store information only in approved systems and avoid unnecessary downloads

7. Data handling and minimisation:
Navigate applies data minimisation in day-to-day work:
• We collect and store only necessary information
• We avoid storing personal data locally where possible
• We limit sharing to those with a legitimate need to know

8. Incident reporting and response:
Any actual or suspected information security incident (including loss of devices, suspected account compromise, or accidental disclosure) must be reported promptly.
Navigate will:
• Assess and contain the incident
• Determine whether personal data is involved
• Follow breach management procedures under our Data Protection & GDPR Policy, including reporting to regulators where required

9. Third-party suppliers:
Where third-party suppliers process or host information for Navigate, we ensure appropriate contractual terms are in place and we take a proportionate approach to supplier due diligence.

10. Responsibilities:
• Leadership is responsible for ensuring appropriate security governance.
• All staff and associates are responsible for following this policy and reporting incidents promptly.

11. Review:
This policy is reviewed at least annually.

12. Contact:
For information security enquiries: gareth@letusnavigate.com