SUPPORTING EDUCATION FOR THE NEXT GENERATION

U-Educate Information Security Policy- December 2025

Organisation: U-educate Ltd (Alternative Provision)
Policy Owner: Christian Brown, Director & Data Protection Officer (DPO)
Approval Date: 05 December 2025
Renewal Date: Annually – next review due 05 December 2026

1. Purpose & Scope

This policy establishes U-educate Ltd's approach to information security in line with ISO/IEC 27001. It applies to all employees, contractors, and third parties handling organisational or client data, including Staffordshire County Council (SCC) information.

2. Acceptable Use

· All IT systems, devices, and data must be used responsibly, lawfully, and only for authorised business purposes.
· Personal use of company systems is permitted only where it does not interfere with business operations or compromise security.
· Prohibited activities include unauthorised software installation, accessing inappropriate content, and sharing confidential data without approval.

3. Access Control

· Access to systems and data is role-based and granted on the principle of least privilege.
· Multi-factor authentication (MFA) is mandatory for administrative and remote access.
· Accounts are reviewed quarterly and revoked immediately upon staff departure.

4. Application Security

· All applications are subject to secure development practices and vulnerability testing.
· Patches and updates are applied promptly following vendor release.
· Third-party applications are assessed for compliance before deployment.

5. Change Control

· All system changes must follow a documented change management process.
· Changes are risk-assessed, tested, and approved before implementation.
· Emergency changes are logged and reviewed retrospectively.

6. Clear Desk & Screen Policy
· Confidential information must not be left unattended on desks or screens.
· Documents must be stored in locked cabinets when not in use.
· Workstations must be locked when unattended.

7. Data Handling
· Personal and sensitive data must be processed in accordance with GDPR and the Data Protection Act 2018.
· Data transfers must be encrypted and logged.
· Retention schedules are enforced; unnecessary data is securely disposed of.

8. Disaster Recovery & Business Continuity
· Daily encrypted backups are taken and tested quarterly.
· Disaster Recovery Plans ensure restoration of critical services within agreed Recovery Time Objectives (RTOs).
· Business Continuity Plans are reviewed annually and tested through scenario exercises.

9. Email Security
· Email accounts are protected by MFA and monitored for phishing attempts.
· Sensitive data must not be transmitted via email unless encrypted.
· Staff are trained to identify and report suspicious emails.

10. Employee Accountability
· All employees are accountable for safeguarding information assets.
· Breaches of this policy are disciplinary offences and may result in termination.
· Responsibilities are outlined in employment contracts and reinforced through training.

11. Encryption
· Encryption is mandatory for data at rest and in transit.
· Full Disk Encryption (FDE) is applied to laptops and removable media.
· Industry-standard protocols (TLS 1.2+, AES-256) are used.

12. Information Classification
· Data is classified as Public, Internal, Confidential, or Restricted.
· Handling requirements are defined for each classification level.
· Restricted data requires explicit authorisation for access.

13. Internet Use
• Internet access is monitored and filtered to prevent malicious activity.
· Business use only; personal browsing must not compromise security.
· Downloading unauthorised software or content is prohibited.

14. Mobile Computing
· Mobile devices must be encrypted, password-protected, and managed via Mobile Device Management (MDM).
· Remote wipe capability is enabled for lost or stolen devices.
· Public Wi-Fi use requires VPN connection.

15. Network Security
· Firewalls, intrusion detection/prevention systems, and anti-malware tools are deployed.
· Network segmentation separates sensitive systems from general access.
· Logs are monitored continuously for anomalies.

16. Physical Security
· Offices are secured with staff passes, CCTV, and visitor logs.
· Servers are housed in UK-based Tier 3 data centres with environmental controls.
· Hardcopy records are stored in locked cabinets with restricted access.

17. Remote Maintenance
· Remote access is restricted to authorised personnel using secure VPN and MFA.
· All remote sessions are logged and monitored.
· Third-party access requires prior approval and contractual safeguards.

18. Secure Disposal
· Electronic media is securely wiped or physically destroyed before disposal.
· Paper records are shredded using cross-cut shredders or secure disposal services.
· Disposal is documented and auditable.

19. Security Awareness & Training
· Mandatory induction and annual refresher training for all staff.
· Training covers data protection, cyber security, breach reporting, and acceptable use.
· Completion is logged and monitored by HR.

20. Risk Management

• Risks are identified, assessed, and recorded in the Information Risk Register.
· Controls are implemented based on ISO27001 Annex A.
· Risk reviews are conducted quarterly and reported to senior leadership.

21. Incident Management

• A formal Incident Response Plan is in place.
· All incidents must be reported immediately to the DPO.
· Incidents are logged, investigated, and corrective actions documented.
· Serious breaches are reported to the ICO within statutory timelines.

22. Policy Review

This policy is reviewed annually or following significant organisational or regulatory changes.
Next Review Date: 05 December 2026

Completed by: Adam Gray
Signature:

Role/Position: Director
Date Completed: 05/12/2025
Review Date: 05/12/2026

U-educate
www.u-educate.co.uk
24, The Courtyard, Gorsey Lane, Coleshill, Birmingham, B46 1JA
Itchen 1, Wallops Wood, Sheardley Lane, Droxford, Southampton, SO32 3QY