United Learning – Information Security Policy

Document Control	
Document Title:	Information Security Policy
Version:	2
Summary of Changes from Previous Version:	Adding information about digital standards and incorporating JCQ guidance.
Name of Originator/Author (including job title):	Jack Treanor, Information Security Officer
Target Audience:	Network Managers and technical staff
Review By Date:	September 2026
Date Issued:	November 2025

Contents

Contents

1. Scope 2
2. Implementation 2
3. Policy Statement 2
4. JQC Guidelines 2
5. Accountability 2
6. Incident Management 3
7. Security Awareness and Training 3
8. United Learning Digital Standards (Cybersecurity) 3
9. Appendix A: PCI/DSS Compliance 5

1. Scope

1.1 The policy and procedure set out in this document apply to all Trustees and Governors, and to all staff employed by United Church Schools Trust ("UCST") and United Learning Trust ("ULT"), including teaching, non-teaching, fixed-term, part-time, full-time, permanent and temporary staff.

1.2 This policy has been updated to include recent policy changes, the release of the United Learning Digital Standards and to reflect updates in the wider threat landscape.

1.3 As a values-led organisation, our values of ambition, confidence, creativity, respect, enthusiasm and determination are key to our purpose and underpin all that we do.

2. Implementation

2.1 Schools must ensure continuous compliance with this policy and comply with digital standards, which is audited through the Technical Assurance Process.

3. Policy Statement

3.1 United Learning is committed to safeguarding all information assets, particularly those containing sensitive or personal data. This policy establishes a framework for protecting the confidentiality, integrity, and availability of information, in compliance with data protection legislation and the organisation's wider duty of care. This policy incorporates and references the United Learning Cyber Security Digital Standards, which set minimum expectations for technology management and information security across all sites.

3.2 Ensure information is protected from unauthorised access. Preserve the confidentiality, integrity, and availability of information. Comply with legal and regulatory requirements. Support business continuity and minimise operational disruption.

4. Joint Council for Qualifications Guidelines

4.1 The JCQ guidelines require that exam sites maintain a cybersecurity policy and follow recommended practices. This policy captures all necessary information to ensure compliance with those guidelines. Where applicable, references to supporting documentation have been included. The controls we have implemented not only meet the JCQ requirements but go beyond them, offering a more comprehensive level of protection.

5. Accountability

5.1 To enable United Learning to defend against cyber threats and demonstrate compliance will implement the following adjacent IT and Data Protection policies, procedures and standards, maintaining appropriate records as required by these procedures:

5.1.1 ICT and AI Acceptable Usage Policy

5.1.2 Data Protection Policy

5.1.3 Data Sharing Policy and Procedure

5.1.4 Clear Desk Policy

5.1.5 Data Protection Impact Assessment policy, procedure and guidance

5.1.6 Security of Personal Data policy

5.1.7 Password Policy

5.1.8 Accessing United Learning Data Using Your Own Device Policy

6. Incident Management

6.1 All security incidents must be reported to Central Office immediately using the cybersecurity@unitedlearning.org.uk and the local IT team.

- Incidents will be investigated by the central office and, where necessary, reported to regulators (ICO).
- If deemed necessary, policies and processes will be reviewed/updated to avoid a similar incident in the future, and to determine whether additional safeguards are required in the environment where the incident occurred, or for the institution.

6.2 See the Data Security Breach Policy for detailed procedures, and for guidance on containing an account compromise, refer to the Investigation Procedures guidance.

6.2.1 Account Compromise Procedure.

6.2.2 Cyber Incident Response Playbook.

7. Security Awareness and Training

7.1 United Learning is committed to maintaining a high level of security awareness across all staff. To support this, the following must be adopted to ensure the protection of sensitive data and compliance with regulatory requirements.

7.2 All employees and contractors are required to complete annual refresher training, which includes:

7.2.1 **The National Cyber Security Centre (NCSC)** training for all employees, as mandated by the **Risk Protection Arrangement (RPA).**

- Data protection training to ensure compliance with the UK GDPR and other applicable legislation.

7.3 All new starters must complete induction training.

7.4 All training resources and records are centrally managed and accessible via the Information Security and Data Protection Hub Page. This hub serves as the single source of truth for training materials, completion tracking, and training records.

8. United Learning Digital Standards (Cybersecurity)

United Learning has adopted the following mandatory digital standards. Each school must implement these per the standard provided (all relevant information security standards are linked below):

8.1 **Anti-Virus Standard**

8.1.1 All endpoints and servers must run approved anti-virus software with automatic updates enabled.

8.2 **Conditional Access Standard**

8.2.1 Access to cloud services must be conditional based on user identity, device health, and location.

8.3 **Data Backup Standards**

8.3.1 Regular, automated backups must be performed and tested. Critical data must be stored securely off-site or in a resilient cloud environment.

8.4 **Firewall Standard**

8.4.1 Network perimeters must be protected by managed firewalls. Rules should follow a deny-all-allow-by-exception principle.

8.5 **Hardware Firmware Standard**

8.5.1 All hardware must run supported firmware versions. Firmware updates must be applied promptly.

8.6 **Internet Filtering Standard**

8.6.1 Web filtering must be enforced for all internet access points. Blocklists and allowlists should reflect educational and safeguarding priorities.

8.7 **Multi-Factor Authentication (MFA) Standard**

8.7.1 MFA must be enabled for all staff access to email, administrative systems, and remote services.

8.8 **Network Standard**

8.8.1 All networks must be segmented by function. Guest networks must be isolated from internal systems.

8.9 **Operating System Standard**

8.9.1 All operating systems must be supported and patched regularly. Unsupported OS must be decommissioned.

8.10 **Password Standard**

8.10.1 Passwords must meet minimum complexity requirements and be changed regularly. Password managers are recommended.

8.11 **USB Standard**

8.11.1 Use of USB storage devices must be restricted and encrypted. Approval must be sought before connecting external media.

8.12 **Account Creation Standard**

8.12.1 Defines the required processes and controls for creating, modifying, and removing user accounts to ensure secure access management and auditability.

8.13 **Application Management and Updating Standard**

8.13.1 Outlines the procedures for securely managing software applications, including installation, configuration, and timely updates to mitigate vulnerabilities.

8.14 **Asset Register Standard**

8.14.1 Establishes the requirements for maintaining an up-to-date and accurate register of all information assets to support risk management and accountability.

8.15 Compliance with these standards will be audited through the Technological Assurance Process.

Appendix

9. Appendix A: PCI/DSS Compliance

United Learning processes card payments exclusively via telephone and uses third-party suppliers for payment services. To ensure compliance with the Payment Card Industry Data Security Standard (PCI/DSS), the following controls must be observed:

9.1.1 Phone Payment Security

Cardholder data must be protected during phone transactions using secure, encrypted methods.

Employees must only access cardholder data if their role requires it, and access must be authorised and logged.

Cardholder data must be masked when displayed (only first 6 or last 4 digits visible).

Full PAN, CVV/CVC, magnetic stripe data, and PINs must never be stored.

9.1.2 Supplier Compliance

All suppliers involved in payment processing must be level 2 PCI/DSS compliant as a minimum.

A written agreement must confirm the supplier's responsibility for protecting cardholder data.

Due diligence must be conducted before engaging suppliers, and their compliance status must be monitored regularly.

PCI/DSS level explained:

Level 1 – Highest Compliance Level

Transaction Volume: Over 6 million card transactions annually (across all channels and brands).

Who It Applies To: Large retailers, global corporations, major e-commerce platforms, and any merchant that has suffered a data breach.

Requirements:

- Annual on-site assessment by a Qualified Security Assessor (QSA).

- Quarterly network vulnerability scans by an Approved Scanning Vendor (ASV).

- Annual Report on Compliance (ROC) and Attestation of Compliance (AOC).

- Penetration testing and detailed documentation of security controls.

Level 2

Transaction Volume: Between 1 million and 6 million card transactions annually.

Who It Applies To: Mid-sized businesses and regional chains.

Requirements:

- Annual Self-Assessment Questionnaire (SAQ) or on-site assessment.

- Quarterly ASV scans.

- May require penetration testing, depending on the payment environment.

Level 3

Transaction Volume: Between 20,000 and 1 million e-commerce transactions annually.

Who It Applies To: Smaller online merchants.

Requirements:

- Annual SAQ.

- Quarterly ASV scans.

- May have reduced requirements depending on the payment method used (e.g., SAQ A-EP vs. SAQ D).

Level 4 – Lowest Compliance Level

Transaction Volume: Fewer than 20,000 e-commerce transactions or up to 1 million total transactions annually.

Who It Applies To: Small businesses and startups.

Requirements:

- Annual SAQ.

- ASV scans if the merchant has an externally facing IP and accepts unencrypted card data.

9.1.3 Device and Data Handling

Locations must maintain a list of all devices used to accept card payments, including make, model, serial number, and location (see Appendix B).

Devices must be inspected regularly for tampering, and staff must be trained to report suspicious activity.

Media containing cardholder data must be securely handled and destroyed when no longer needed.

9.1.4 Incident Response

Any suspected breach involving cardholder data must be reported immediately to the Central Finance Team.

The Central Office team will investigate, mitigate risks, and report findings to relevant parties.