Huish Episcopi Academy
The best in everyone™
Part of United Learning

Information Security Policy

United Learning Information Security Policy

Scope

The policy and procedure set out in this document applies to all United Church Schools Trust (UCST) and United Learning Trust (ULT) teaching and support staff; including fixed-term, part-time, full-time, permanent and temporary staff. The two companies (UCST and ULT) are referred to in this policy by their trading name, 'United Learning'.

Where this policy refers to 'School' or 'Head Teacher', within Central Office this should be interpreted to refer to the department where a member of staff works and their Head of Department.

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.

This Policy Document when read in conjunction with the ICT Acceptable Use Policy encompasses all aspects of security relating to the handling of sensitive information (including personal and company information).

For those staff who handle credit/debit card payments (payment card processing) it also covers the handling of information as required for PCI/DSS.

All Company employees must read this document and sign United Learning's ICT Acceptable Use Policy confirming they have read and understand this policy fully. *Only staff involved in payment card processing need to read the appendices on PCI/DSS.*

Dated: 27/07/2020

Contents

Information Security Policy 4

1. Acceptable Use Policy 4
2. Information Classification 4
3. Physical Security 5
4. Protection of Data in Transit 5
5. Disposal of Stored Data 5
6. Security Awareness and Procedures 6
7. Security Incident Response Plan 6
8. Transfer of Sensitive Information Policy 7
9. User Access Management 7
10. Access Control Policy 7

Appendix A – PCI/DSS 10

1. Network Security 10
2. For employees with Access to the Sensitive Cardholder Data 10
3. Protect Stored Data 11
4. Protect Data in Transit 11
5. Disposal of Stored Data 11
6. Security Awareness and Procedures 11
7. PCI Incident Response Plan 11
9. Transfer of Sensitive Information Policy 13

Appendix B – List of Devices 13

Appendix C - List of Service Providers 14

Appendix D – VISA breach reporting requirements 15

Appendix E - Mastercard breach reporting requirements 16

Appendix F - American Express breach reporting requirements 17

1. Information Security Policy

United Learning handles sensitive information daily. Sensitive information must have adequate safeguards in place to protect the data, privacy, and to ensure compliance with various regulations, along with guarding the future of the organisation.

United Learning commits to respecting the privacy of all its clients (including parents/carers and pupils) and employees and to protecting any client data from outside parties. To this end management are committed to maintaining a secure environment in which to process client information so that we can meet these promises.

Employees handling sensitive information should ensure they:

- handle Company information in a manner that fits with their sensitivity and classification.
- limit personal use of United Learning information and telecommunication systems and ensure it doesn't interfere with your job performance.
- do not disclose personal information unless authorised.
- request approval from management prior to establishing any new software or hardware, third party connections, etc.
- do not install unauthorised software or hardware, including wireless access unless you have explicit management approval.
- always leave desks clear of sensitive data and lock computer screens when unattended.
- store United Learning information securely and protect against unauthorised use at all times. Any sensitive data that is no longer required by United Learning for business reasons must be destroyed in a secure and irrecoverable manner.
- report Information Security incidents, without delay, to the individual responsible for incident response locally and to cybersecurity@unitedlearning.org.uk.

2. Acceptable Use Policy

The Central Office Acceptable Use Policy will apply within Central Office; Schools will have their own Acceptable Use Policy

3. Information Classification

Data will be labelled and controlled in accordance with the Protective Marking policy

- **Confidential data** might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to United Learning if disclosed or modified. **Confidential data includes cardholder data**.
    - Information containing personal data is a subset of confidential data

- **Internal Use data** might include information that the data owner feels should be protected to prevent unauthorised disclosure.
- **Public data** is information that may be freely disseminated.

4. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- Media is defined as any printed or handwritten paper, received faxes, back-up tapes, computer hard drive, etc.
- Strict control is maintained over the external or internal distribution of any media and has to be approved by management.
- Strict control is maintained over the storage and accessibility of media
- Visitors must always be escorted by a trusted employee.
    - Exceptions may be made on a case by case, site by site basis and subject to an appropriate risk assessment to allow some visitors to be unescorted (e.g. regular visitors who have undergone an induction and have a DBS - counsellors etc.)
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. "Employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are "resident" on United Learning sites. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to physically enter the premises for a short duration, usually not more than one day.
- United Learning staff should verify the identity of any third-party personnel claiming to repair or run maintenance tasks on any devices, install new devices or replace devices.

5. Protection of Data in Transit

All sensitive data must be protected securely if it is to be moved physically or electronically.

- If there is a business justification to send data via email or by any other mode then it should be done after authorisation and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, etc. more information is widely available on the internet – for example https://www.proofpoint.com/uk/glossary/encryption).
- The transportation of media containing sensitive data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier/postal services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

6. Disposal of Stored Data

- All data must be securely disposed of when no longer required by United Learning, regardless of the media or application type on which it is stored.
- An automatic process must exist to permanently delete on-line data, when no longer required.

- United Learning sites must have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- United Learning sites must have documented procedures for the destruction of electronic media. These will require:
    - All data on electronic media to be rendered unrecoverable when deleted e.g. through degaussing or electronically wiping using military grade secure deletion processes or the physical destruction of the media.
    - If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.
    - Data must only be deleted in accordance with the records retention schedule.

7. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.
- All employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with United Learning.
- Company security policies must be reviewed annually and updated as needed.

8. Security Incident Response Plan

- United Learning Data Breach/Security Incident response plan is as follows:

1. Each department/school must report an incident to the Data Protection Lead (or in their absence the Head/Principal or the IT Manager) for breach reporting.

2. The incident will be investigated by the Information Security Officer or the Company Secretariat team within Central Office or by local school staff with responsibility in this area.

3. If deemed necessary, the incident will be reported to the ICO.

4. 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.

5. For more detail refer to the data security breach policy.

9. Transfer of Sensitive Information Policy

- All third-party companies providing critical services to United Learning must provide an agreed Service Level Agreement.
- All third-party companies providing hosting facilities will comply with United Learning's Physical Security and Access Control Policy

10. User Access Management

- Access to United Learning systems is controlled through a formal user registration process beginning with a formal notification from HR.
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions.
- There is a standard level of access; other services can be accessed when specifically authorised by HR/line management.
- The job function of the user decides the level of access the employee has to cardholder data; *most employees will not need access to any cardholder data, others may require cardholder name while others may require cardholder name and parts of the Permanent Account Number (PAN).*
- A request for service must be made in writing (email/form or hard copy) by the newcomer's line manager or by HR. The request can be free format, but must state:

  Name of person making request.
  Job title of the newcomers and workgroup.
  Start date.
  Services required.

- Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure. The user signs the form indicating that they understand the conditions of access.
    - Annual Renewal and ICT Acceptable Use are in addition to this.
- Access to all United Learning systems is provided by IT and can only be started after proper procedures are completed.

- As soon as an individual leaves United Learning employment, all his/her system logons must be immediately revoked.
- As part of the employee termination process HR (or line managers in the case of contractors) will inform IT of all leavers and their date of leaving.

11. Access Control Policy

- Access Control systems are in place to protect the interests of all users of United Learning computer systems by providing a safe, secure and readily accessible environment in which to work.

- United Learning will provide all employees and other users with the information they need to carry out their responsibilities in an as effective and efficient manner as possible.
- Generic or group IDs shall not normally be permitted but may be granted under exceptional circumstances if sufficient other controls on access are in place. Approval shall be sought from an appropriate level of management; within Central Office this will be from the 'PCI Silver Team'.[1]
- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorisation provided jointly by the system owner and IT Services. Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification and has the express written prior approval of management.
- Users are obligated to report instances of non-compliance to the DPL/IT Services.
- Access to United Learning IT resources and services will be given through the provision of a unique Active Directory account and complex password.
- Access to any United Learning IT resources and services will not be provided without prior authentication and authorisation of a user's requirement for a United Learning Windows Active Directory account from Human Resources.
- Password issuing, strength requirements, changing and control will be managed through formal processes. Password length, complexity and expiration times will be controlled through Windows Active Directory Group Policy Objects or other software offering the same level of control.
- Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the relevant manager or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.
- Users are expected to become familiar with and abide by United Learning policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
- Access for remote users shall be subject to authorisation by IT Services and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.
- Access to data is variously and appropriately controlled according to the data classification levels described in the Protective Marking Policy.
- Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks and other methods as necessary.

[1] A virtual group comprising the Director of IT, Head of Schools' IT Strategy, Service Desk Manager, Systems Manager and Information Security Officer

- A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users' access rights. The review shall be logged, and IT Services shall sign off the review to give authority for users' continued access rights.

12. Appendix A – PCI/DSS

In addition, employees handling payment cards/payment card information should ensure:

- They take extra care to protect sensitive cardholder information.

Everyone has a responsibility for ensuring United Learning's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the information detailed herein you should seek advice and guidance from your line manager.

1. Network Security

A high-level network diagram is maintained and reviewed on a yearly basis. Where applicable the network diagram provides a high-level overview of the cardholder data environment (CDE), which at a minimum shows the connections in and out of the CDE. Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable should also be illustrated.

2. For employees with Access to the Sensitive Cardholder Data

All Access to sensitive cardholder should be controlled and authorised. Any job functions that require access to cardholder data should be clearly defined.

- Any display of the card holder should be restricted at a minimum to the first 6 or the last 4 digits of the cardholder data.
- Access to sensitive cardholder information such as PANs, personal information and business data is restricted to employees that have a legitimate need to view such information.
- No other employees should have access to this confidential data unless they have a genuine business need.
- If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained (for each location) as detailed in Appendix C - List of Service Providers
- United Learning will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the cardholder data that the Service Provider possesses.
- United Learning will ensure that a there is an established process, including proper due diligence is in place, before engaging with a Service provider.
- United Learning will have a process in place to monitor the PCI DSS compliance status of the Service provider.

- Each location shall maintain a list of devices that accept payment card data. (see Appendix B – List of Devices**Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.**)
- The list should include make, model and location of the device and should have the serial number or a unique identifier of the device
- The list should be updated when devices are added, removed or relocated
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.

- POS device surfaces are periodically inspected to detect tampering or substitution.
- Personnel using the devices should be trained and aware of handling the POS devices
- Personnel using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel.
- All computers that access sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

3. Protect Stored Data

- If there is no specific need to see the full PAN (Permanent Account Number), it must be masked when displayed.

It is strictly prohibited to store:

- **The contents of the payment card magnetic stripe (track data) on any media whatsoever.**
- **The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.**
- **The PIN or the encrypted PIN Block under any circumstance.**

4. Protect Data in Transit

- Card holder data (PAN, track data, etc.) must never be sent over the internet via email, instant chat or any other end user technologies.

5. Disposal of Stored Data

All cardholder information must be destroyed as soon as it is no longer required; if this is not possible and it is awaiting destruction it must be held in lockable storage containers clearly marked “To Be Shredded” - access to these containers must be restricted.

All hard copies of cardholder data must be manually destroyed when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.

6. Security Awareness and Procedures

- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).

7. PCI Incident Response Plan

- United Learning PCI security incident response plan is as follows:

    - Upon receiving a report from the Data Protection Lead (or other applicable member of staff) of a breach the PCI Response Team will be advised.
    - Members of the PCI Response Team will investigate the incident and assist the potentially compromised department in limiting the exposure of cardholder data and

in mitigating the risks associated with the incident.

- The PCI Response Team will ensure the problem is resolved to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.
- The PCI Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.

United Learning PCI Security Incident Response Team:

Chief Operating Officer
Chief Financial Officer
Financial Controller
Company Secretary
Group IT Systems Manager
Information Security Officer

Information Security PCI Incident Response Procedures:

- A department or school that reasonably believes it may have an account breach, or a breach of cardholder information or of systems related to the PCI environment in general, must inform United Learning PCI Incident Response Team. After being notified of a compromise, the PCI Response Team, along with other designated staff, will implement the PCI Incident Response Plan to assist and augment department/school's response plans.

Incident Response Notification

Escalation Members:

Escalation – First Level:
Information Security
Officer
Others to be assigned

Escalation – Second Level:
To be assigned

External Contacts (as needed)
Merchant
Provider Card
Brands
Internet Service Provider (if applicable)
Internet Service Provider of Intruder (if applicable)
Insurance Carrier
Law Enforcement Agencies as applicable in local jurisdiction

In response to a systems compromise, the PCI Response Team and designees will:

1. Ensure compromised system/s is isolated on/from the network.
2. Gather, review and analyse the logs and related information from various central and local safeguards and security controls

3. Conduct appropriate forensic analysis of compromised system.
4. Contact internal and external departments and entities as appropriate.
5. Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
6. Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.

Points 2 and 3 above may require suitably qualified personnel to be contracted in.

The credit card companies have individually specific requirements that the Response Team must address in reporting suspected or confirmed breaches of cardholder data. See appendices (D-F) below for these requirements.

9. Transfer of Sensitive Information Policy

- All third-party companies which have access to Card Holder information must

1. Adhere to the PCI DSS security requirements.
2. Acknowledge their responsibility for securing the Card Holder data.
3. Acknowledge that the Card Holder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
4. Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.
5. Provide full cooperation and access to conduct a thorough security review after a security intrusion by a Payment Card industry representative, or a Payment Card industry approved third party.

13.

14. Appendix B – List of Devices

Asset/Device Name	Description	Owner/Approved User	Location

15. Appendix C - List of Service Providers

Name of Service Provider	Contact Details	Services Provided	PCI DSS Compliant	PCI DSS Validation Date

16. Appendix D – VISA breach reporting requirements

VISA Steps

If the data security compromise involves credit card account numbers, implement the following procedure:

- Shut down any systems or processes involved in the breach to limit the extent and prevent further exposure.
- Alert all affected parties and authorities such as the Merchant Bank (your Bank), Visa Fraud Control, and the law enforcement.
- Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.
- For more Information visit: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_ compromised.html

Visa Incident Report Template

This report must be provided to VISA within 14 days after initial report of incident to VISA. The following report content and standards must be followed when completing the incident report. Incident report must be securely distributed to VISA and Merchant Bank. Visa will classify the report as "VISA Secret" *.

I. Executive Summary
   a. Include overview of the incident
   b. Include RISK Level (High, Medium, Low)
   c. Determine if compromise has been contained
II. Background
III. Initial Analysis
IV. Investigative Procedures
   a. Include forensic tools used during investigation
V. Findings
   a. Number of accounts at risk, identify those stores and compromised
   b. Type of account information at risk
   c. Identify ALL systems analysed. Include the following:
      - Domain Name System (DNS) names
      - Internet Protocol (IP) addresses
      - Operating System (OS) version
      - Function of system(s)
   d. Identify ALL compromised systems. Include the following:
      - DNS names
      - IP addresses
      - OS version
      - Function of System(s)
   e. Timeframe of compromise
   f. Any data exported by intruder
   g. Establish how and source of compromise
   h. Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments, data on software engineers' machines, etc.)
   i. If applicable, review VisaNet endpoint security and determine risk

VI. Compromised Entity Action
VII. Recommendations
VIII. Contact(s) at entity and security assessor performing investigation

*This classification applies to the most sensitive business information, which is intended for use within VISA. Its unauthorized disclosure could seriously and adversely impact VISA, its employees, member banks, business partners, and/or the Brand.

17. Appendix E - Mastercard breach reporting requirements

MasterCard Steps:

I. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 0800-96-4767.
II. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to compromised_account_team@mastercard.com.
III. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
IV. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
V. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
VI. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
VII. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.

2. Distribute the account number data to its respective issuers.

Employees of United Learning will be expected to report to the security officer for any security related issues. The role of the security officer is to effectively communicate all security policies and procedures to employees within United Learning and contractors. In addition to this, the security officer will oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in both this document and at the training sessions and finally, oversee the implantation of the incident response plan in the event of a sensitive data compromise.

18. Appendix F - American Express breach reporting requirements

American Express Steps

I. Within 24 hours of an account compromise event, notify American Express Merchant Services at 01273 67 55 33 in the U.K.
II. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
III. Prepare a list of all known compromised account numbers Obtain additional specific requirements from American Express

Prepared by M Wood:	October 2023
Ratified by Governors:	October 2023
To be reviewed:	October 2024