Data Security Policy

Document Reference:	HTC-POL-OPS-003
Policy Owner:	Chief Operating Officer
Approved By:	Group Chief Executive Officer
Version:	2.0
Effective Date:	January 2026
Review Date:	January 2027

Version Control

Version	Date	Author	Changes
1.0	08/08/2024	Sophie Gilmore	Initial policy creation
1.1	29/08/2025	Patsy Crocker	Reviewed for completeness
2.0	Jan 2026	Sophie Gilmore	Major revision: enhanced password standards, cyber security section, incident response procedures, mobile device security, remote working guidance

1. Purpose

This Data Security Policy establishes the standards and procedures for protecting Hybrid Training Centre's (HTC) information assets. All forms of data are company assets, and their loss or misuse can be costly, damaging to reputation, and in some cases unlawful.

The policy aims to:

- Protect information from unauthorised access, disclosure, modification, or destruction
- Ensure the confidentiality, integrity, and availability of information systems
- Comply with legal, regulatory, and contractual requirements (including UK GDPR and ESFA requirements)
- Maintain the trust of learners, employers, and other stakeholders
- Support business continuity by protecting critical information assets

2. Scope

This policy applies to:

- All HTC employees, contractors, and temporary staff
- All information processed by HTC (electronic and paper-based)
- All IT systems, devices, and networks (including cloud services)
- HTC premises and remote working locations
- Third-party suppliers with access to HTC systems or data

The policy covers information relating to learners, apprentices, staff, employers, and business operations.

3. Information Classification

HTC classifies information according to its sensitivity and the impact of unauthorised disclosure:

Classification	Description	Examples
Confidential	Highly sensitive; disclosure would cause significant harm	Personal data, financial records, safeguarding records
Internal	For internal use only; not for external sharing without authorisation	Policies, meeting minutes, operational data
Public	May be shared externally without restriction	Marketing materials, published policies

All information should be handled according to its classification. When in doubt, treat information as Confidential.

4. User Access Control

4.1 User Authorisation

- Access to HTC systems must be formally authorised by a Director or line manager
- Each user is assigned a unique user identity (username)
- Access rights are granted based on the principle of least privilege (minimum access needed for the role)
- Access rights are reviewed when staff change roles and revoked immediately upon leaving

4.2 Password Standards

All users must comply with the following password requirements:

- Minimum 12 characters in length
- Combination of uppercase, lowercase, numbers, and special characters
- Must not contain personal information (name, date of birth, etc.)
- Must not be a common dictionary word or phrase
- Must not be reused across different systems
- Must be changed immediately if compromise is suspected
- Must be changed every 90 days (or 60 days for administrator accounts)
- Must never be shared with anyone, including IT staff or managers

4.3 Multi-Factor Authentication (MFA)

Multi-factor authentication is required for:

- Remote access to HTC systems
- Access to systems containing personal or financial data
- Administrator and privileged accounts
- Cloud services (Office 365, OneFile, etc.)

4.4 Account Management

- User accounts are suspended after 5 consecutive failed login attempts
- Inactive accounts are disabled after 90 days without use
- Accounts are disabled immediately when employment ends
- Password resets require identity verification

5. Physical Security

5.1 Premises Security

- Access to HTC premises is controlled (key fobs, locks, visitor sign-in)
- Visitors must be signed in and accompanied in secure areas
- Server rooms and network equipment are in locked areas with restricted access

5.2 Clear Desk and Clear Screen

- Confidential documents must not be left unattended on desks
- Paper documents must be stored in locked cabinets when not in use
- Computer screens must be locked when leaving the workstation (Windows+L or Ctrl+Alt+Delete)
- Automatic screen lock activates after 5 minutes of inactivity

5.3 Secure Disposal

- Paper documents containing personal or confidential data must be shredded (cross-cut)
- Confidential waste bins are provided for secure disposal
- IT equipment must be securely wiped before disposal or transfer
- Hard drives are destroyed or securely wiped using certified software

6. Device Security

6.1 HTC-Owned Devices

- All HTC laptops and computers have antivirus software installed and updated
- Operating systems and software are kept up to date with security patches
- Firewalls are enabled on all devices
- Full disk encryption is enabled on all laptops
- Only authorised software may be installed

6.2 Personal Devices (BYOD)

Use of personal devices for HTC work is only permitted with approval and must comply with the following:

- Device must have a passcode/PIN lock
- Device must have up-to-date antivirus software (where applicable)
- HTC data must not be stored locally on personal devices
- Lost or stolen devices must be reported immediately

6.3 Removable Media

- Use of USB drives and removable media is discouraged
- Where necessary, only HTC-approved encrypted USB drives may be used
- Personal USB drives must not be connected to HTC devices
- Data on removable media must be encrypted

7. Network and Internet Security

7.1 Network Protection

- HTC networks are protected by firewalls

- Network traffic is monitored for suspicious activity
- WiFi networks are encrypted (WPA3 or WPA2 minimum)
- Guest WiFi is segregated from the corporate network

7.2 Internet Use

- Internet access is provided for business purposes
- Limited personal use is permitted during breaks
- Users must not access illegal, offensive, or inappropriate content
- Downloads from untrusted sources are prohibited
- Streaming services should not be used excessively (bandwidth)

7.3 Public WiFi

When working remotely:

- Avoid using public WiFi for accessing HTC systems where possible
- If public WiFi must be used, connect via VPN
- Never access sensitive data on unsecured networks

8. Email Security

- Be cautious of unexpected emails, especially those with attachments or links
- Verify the sender before clicking links or opening attachments
- Report suspicious emails (phishing) to IT immediately
- Do not send confidential information via unencrypted email
- Use secure file transfer methods for sensitive documents
- Check recipient addresses carefully before sending (avoid misdirected emails)

9. Remote Working Security

Staff working remotely must ensure:

- A secure home working environment (screens not visible to others)
- Use of VPN when accessing HTC systems remotely
- Secure storage of any paper documents taken home
- No use of shared or public computers for HTC work
- Confidential phone calls are not overheard
- Work devices are not left unattended in vehicles
- Home WiFi is secured with a strong password

10. Cyber Security Awareness

All staff must be aware of common cyber threats:

10.1 Phishing

Fraudulent emails designed to trick recipients into revealing information or clicking malicious links. Warning signs include unexpected emails, urgency, spelling errors, and suspicious links.

10.2 Ransomware

Malicious software that encrypts files and demands payment. Never pay ransoms. Report immediately and disconnect affected devices from the network.

10.3 Social Engineering

Manipulation techniques to trick people into revealing confidential information. Be suspicious of unexpected requests for information, even from apparent colleagues or IT support.

11. Security Incident Reporting

All security incidents or suspected incidents must be reported immediately to the COO and IT. Examples include:

- Lost or stolen devices
- Suspected virus or malware infection
- Phishing emails received or clicked
- Unauthorised access to systems or data
- Unusual system behaviour
- Misdirected emails containing personal data

Early reporting enables rapid response and minimises damage. There is no penalty for reporting incidents in good faith.

12. Assessment Records Security

Specific requirements for learner assessment documentation:

- Electronic assessment records are stored on OneFile/secure platforms with role-based access
- Paper-based assessment records are stored in locked cabinets in each curriculum area
- Lead IQAs are responsible for the security of assessment documentation
- Assessment records must be maintained for a minimum of 6 years following certification
- Verified and certificated records are scanned and stored electronically

13. Responsibilities

13.1 All Users

- Follow this policy and related procedures
- Protect passwords and access credentials
- Report security incidents or weaknesses immediately
- Complete required security training
- Only access data necessary for their role

13.2 Line Managers

- Ensure team members understand and comply with this policy
- Authorise appropriate access for team members
- Report leavers immediately to IT for access removal
- Ensure new starters complete security training

13.3 IT Support / System Administrators

- Maintain technical security controls
- Monitor systems for security incidents
- Manage user access and accounts
- Ensure backups are performed and tested

- Keep systems patched and updated

13.4 COO (Policy Owner)

- Overall responsibility for data security
- Monitoring compliance with this policy
- Managing security incident responses
- Ensuring adequate training is provided

14. Monitoring

HTC reserves the right to monitor use of IT systems to ensure compliance with this policy and protect information assets. Monitoring may include:

- Internet usage patterns
- Email communications
- File access logs
- System login records

Monitoring is conducted in accordance with applicable laws and the HTC Privacy Notice.

15. Breach of Policy

Breach of this policy may result in:

- Disciplinary action up to and including dismissal
- Criminal prosecution (where applicable)
- Civil action for damages

Deliberate circumvention of security controls is considered gross misconduct.

16. Related Documents

- Data Protection and GDPR Policy
- IT Acceptable Use Policy
- Business Continuity Plan
- Remote Working Policy
- Social Media Policy
- Disciplinary Policy

17. Monitoring and Review

This policy is reviewed annually by the COO or sooner if required by changes to technology, threats, or regulatory requirements.

Policy Approval

Signature: Date:

Sophie Gilmore
Group Chief Executive Officer