(NOTE: Throughout this document, THE TEACHER TRAINER LTD is referred to as TTT)

TTT POLICY DOCUMENT

Information Security and Cyber Security Policy

Protecting TTT systems and data from loss, compromise and unauthorised access.

Document Control

Document Title	Information Security and Cyber Security Policy
Version	1.0
Effective Date	22 April 2026
Next Review Date	22 April 2027
Policy Owner	Phenil Mehta, Centre Manager
Security Incident Contact	phenil@theteachertrainer.co.uk, 01908 736 777
Approved By	Phenil Mehta, Centre Manager
Classification	Public
Applies To	All TTT staff, associates, resellers, processors and third parties with access to TTT systems or data

The Teacher Trainer Ltd | Regus House, Fairbourne Drive, Atterbury, Milton Keynes MK10 9RG
01908 736 777 | info@theteachertrainer.co.uk | www.theteachertrainer.co.uk

Information Security and Cyber Security Policy

1. Purpose

This policy sets out the technical and organisational measures TTT applies to protect its systems, data and services from loss, compromise and unauthorised access. It supports compliance with the UK GDPR's security principle (Article 32), the Data Protection Act 2018 and Awarding Organisation centre requirements. The policy is designed around the principles of the Cyber Essentials scheme and the National Cyber Security Centre's (NCSC) Small Business Guide.

2. Scope

This policy applies to:

- All TTT staff, associates and contractors who access TTT systems or data
- Resellers, processors and suppliers with access to TTT data, in line with their contracts
- All devices used for TTT work, whether owned by TTT or by the individual (BYOD)
- All systems used by TTT, including the Learning Management System (LMS), email, file storage, finance and messaging platforms
- All network connections, remote access and cloud services

3. Definitions

The following terms carry the meanings given throughout this policy.

Information Security	The confidentiality, integrity and availability of TTT information.
Cyber Security	The protection of TTT systems and data from digital attack and unauthorised access.
Access Control	The technical and administrative measures that determine who can access what information and system.
Multi-Factor Authentication (MFA)	A method of authentication requiring two or more independent factors, such as a password plus a code from an authenticator app.
BYOD	Bring Your Own Device. The use of a personal device to access TTT systems or data.
Security Incident	Any event that has compromised or could compromise, the confidentiality, integrity or availability of TTT information or systems.
Phishing	An attempted attack using deceptive email, SMS or calls to trick someone into disclosing credentials or other sensitive information.

4. Policy Statement

TTT is committed to the following principles and commitments.

1. Information security is everyone's responsibility; every staff member, associate and supplier is accountable for applying this policy.
2. TTT applies the Cyber Essentials control themes (firewalls, secure configuration, user access control, malware protection, patch management) as its baseline.
3. Access to TTT systems and data is granted on a least-privilege, need-to-know basis and reviewed regularly.
4. Multi-factor authentication is enforced on every system that supports it, starting with email, the Learning Management System (LMS), finance systems and cloud storage.
5. Personal data in transit is protected by current Transport Layer Security (TLS); personal data at rest in supplier systems is encrypted where the supplier offers it.
6. Suspected security incidents are reported without delay and handled under Section 12.
7. TTT's security posture is reviewed at least annually and after any significant system, supplier or threat-landscape change.

5. Roles and Responsibilities

Role	Responsibility
Centre Manager (Phenil Mehta)	Overall accountability; authorises system access; signs off supplier security assessments; leads incident response; approves any deviation from this policy.
Course Coordinator	Day-to-day administration of access and account joiners/leavers; applies policy to new associates; maintains asset and supplier register.
All staff, associates and contractors	Comply with this policy and associated procedures; complete required training; report suspected incidents immediately.
Processors and suppliers	Meet the security terms of their TTT contract; support TTT's incident response; notify breaches to TTT without undue delay.

6. Access Control

- Every user has a unique named account; shared accounts are not permitted
- Access is granted on a least-privilege basis and documented in the Access Register
- Administrative privileges are separated from day-to-day user accounts
- Access for staff, associates and contractors is removed within one working day of their leaving or their role ending
- Access is reviewed quarterly; dormant accounts are disabled
- Third-party access is time-limited and logged

7. Authentication and Passwords

- Passwords follow NCSC guidance: a minimum of 12 characters where possible, no reuse of personal passwords; no sharing
- Multi-factor authentication is enforced wherever the system supports it; authenticator apps are preferred to SMS
- Users to avoid repeated re-entry of credentials on links received by email or message
- Credentials are stored in a reputable password manager, not in plain text, on paper or in browser autofill without MFA

8. Device and Endpoint Security

- Every device used for TTT work has: a supported operating system; a reputable anti-malware product; automatic updates enabled; disk encryption enabled; a strong device passcode or biometric lock
- Mobile devices lock automatically after no more than 5 minutes of inactivity
- Lost or stolen devices are reported to the Centre Manager immediately; remote lock or wipe is initiated where available
- Personal devices used under BYOD meet the same standards; the user consents to TTT's right to require data removal at end of engagement
- Removable media (USB sticks, memory cards) are used only where unavoidable and are encrypted
- Devices at end of life are wiped or destroyed in line with the Data Retention and Disposal Policy

9. Network, Cloud and Email

- TTT uses reputable, UK- or EU-hosted cloud services wherever possible and records international transfer safeguards
- Home and mobile networks used for TTT work use strong Wi-Fi passwords, updated router firmware and WPA2 or WPA3 encryption
- Public Wi-Fi is not used for access to TTT systems unless through a reputable VPN
- TTT email uses reputable services (Zoho Mail or Google Mail or Microsoft Outlook) with DMARC, DKIM and SPF to reduce spoofing; external-sender warnings are enabled where the provider supports them
- Auto-forwarding from TTT email to external addresses is blocked by default

10. Patching and Backups

- Operating systems, applications and firmware are patched within 14 days of a fix being released for a high or critical vulnerability
- Unsupported software is not used; where an exception is unavoidable, it is documented with a mitigating control

- Critical TTT data is backed up through the Learning Management System (LMS), cloud storage and finance systems, with supplier-side redundancy
- Backup restoration is tested at least annually for the most critical data categories
- Backups are covered by the Data Retention and Disposal Policy

11. Supplier and Third-Party Security

- New suppliers handling TTT personal data are assessed against this policy before engagement, including review of their security certifications (ISO 27001, SOC 2, Cyber Essentials Plus) where available
- Data processing agreements include security, sub-processor and breach-notification clauses
- Significant incidents at suppliers are reviewed at the point of supplier renewal

12. Security Incidents

1. Any suspected security incident (including phishing emails, unauthorised access, device loss, ransomware, malware or a suspected supplier breach) is reported to the Centre Manager at phenil@theteachertrainer.co.uk or by phone on 01908 736 777 without delay.
2. The Centre Manager contains the incident, assesses impact on TTT data and systems and logs the incident in the Incident Register.
3. Where the incident involves personal data, the Personal Data Breach process under the Data Protection and GDPR Policy is activated (internal within 24 hours of discovery; ICO within 72 hours where the threshold is met).
4. External specialist support is engaged where needed (insurance-appointed responders, NCSC guidance, Police through Action Fraud).
5. A post-incident review identifies root cause and corrective actions and these are tracked to closure.

13. Phishing and Social Engineering

- All staff and associates are trained to recognise phishing indicators and never to enter TTT credentials on a page reached through a link in an email or message
- Unexpected requests for credentials, payments, gift cards or data are verified through a known trusted channel before action
- Phishing attempts are reported to the Centre Manager and the suspect email forwarded to report@phishing.gov.uk

14. Acceptable Use

- TTT systems are used for authorised business purposes; limited and reasonable personal use is permitted but must not breach this policy or TTT's other policies
- Software is installed on TTT-managed devices only from reputable, authorised sources
- Bypass or disabling of security controls is prohibited

- Company information is not shared through unapproved services, personal email, consumer messaging or unmanaged cloud storage

15. Training and Awareness

Audience	Content	Frequency
All staff and associates	Cyber hygiene, phishing, passwords, MFA, incident reporting, acceptable use	Induction and annual refresh
Centre Manager and Course Coordinator	Incident response; supplier security assessment; access reviews	Annual
New joiners	Pre-access briefing covering this policy and account setup	Before first system access

16. Monitoring and Review

This policy is reviewed annually by the Centre Manager as part of TTT's self-evaluation process. Interim reviews are triggered by a significant incident, an NCSC or ICO guidance change, a supplier or system change or a material change to the threat landscape. All outcomes are recorded in the Version History at Section 18.

17. Related Documents

This policy should be read alongside:

- Data Protection and GDPR Policy
- Privacy Notice
- Data Retention and Disposal Policy
- Business Continuity and Disaster Recovery Policy
- Artificial Intelligence Policy
- Online Learning and Digital Conduct Policy
- Social Media Policy
- Electronic Communication Disclaimer Policy
- Cookies Policy
- Safer Recruitment Policy
- Staff Code of Conduct

18. Version History

Version	Date	Author	Summary of Changes
1.0	22/04/2026	Phenil Mehta	A new standalone policy aligned with Cyber Essentials control themes and NCSC Small Business Guide, covering access control, authentication, devices, cloud and email, patching, backups, supplier security, incidents, phishing, acceptable use and training.

19. Approval

This policy has been reviewed and approved by the Centre Manager of TTT.

Phenil Mehta	*P Mehta*	22/04/2026
Name	**Signature**	**Date**