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

TTT POLICY DOCUMENT

Business Continuity and Disaster Recovery Policy

How TTT keeps delivering courses when people, systems or suppliers are disrupted.

Document Control

Document Title	Business Continuity and Disaster Recovery Policy
Version	1.0
Effective Date	22 April 2026
Next Review Date	22 April 2027
Policy Owner	Phenil Mehta, Centre Manager
Incident Command Contact	Phenil Mehta, phenil@theteachertrainer.co.uk, 01908 736 777
Deputy (where CM unavailable)	Shaily Mehta, shaily@theteachertrainer.co.uk
Approved By	Phenil Mehta, Centre Manager
Classification	Public
Applies To	All TTT staff, associates, learners, resellers and critical suppliers

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

Business Continuity and Disaster Recovery Policy

1. Purpose

This policy sets out how TTT keeps delivering courses and meeting its commitments to learners, Awarding Organisations and regulators when a significant disruption occurs. It identifies TTT's critical activities, the disruptions that matter most, the target times within which they must be restored and the actions TTT takes to protect learners and recover services. It is aligned with the principles of ISO 22301 adapted to a small online centre.

2. Scope

This policy applies to:

- All TTT staff, associates, volunteers and contractors
- All TTT systems, including the learning management system, email, file storage, finance and messaging
- All critical suppliers whose failure would materially affect course delivery
- All TTT learners, during a disruption that affects their course

3. Definitions

The following terms carry the meanings given throughout this policy.

Business Continuity	Planned activity that enables TTT to keep delivering critical services during and after a disruption.
Disaster Recovery	The subset of activity focused on restoring technology, systems and data after a failure or loss.
Disruption	Any event that prevents or significantly slows a critical TTT activity, whether caused by people, technology, supplier, premises, utilities or external factors.
Recovery Time Objective (RTO)	The target time within which a critical activity must be restored after a disruption.
Recovery Point Objective (RPO)	The maximum tolerable period of data loss, measured as the most recent usable backup point.
Incident Command Contact	The person who leads TTT's response during an incident, by default the Centre Manager and, if unavailable, the named Deputy.
Invocation	The formal decision that an event is an incident requiring activation of this policy's response procedures.

4. Policy Statement

TTT is committed to the following principles and commitments.

1. Learner continuity is the priority during any disruption; financial and commercial considerations come second.
2. TTT identifies its critical activities, assesses the disruptions that could affect them and puts proportionate controls and recovery plans in place.
3. Targets for recovery (RTO and RPO) are documented and reviewed annually.
4. The incident command structure is clear and rehearsed; staff know who leads in an incident and who deputises.
5. Communication with learners, staff, Awarding Organisations and critical suppliers during a disruption is honest, timely and consistent.
6. Learnings from every incident, rehearsal and near miss are fed back into the policy and plans.

5. Critical Activities and Recovery Targets

TTT's critical activities, the maximum time they can be offline before learners or regulators are meaningfully affected (RTO) and the maximum data loss TTT can tolerate (RPO) are as follows.

Critical Activity	RTO	RPO	Dependencies
Learner access to the LMS (submissions, feedback, materials)	3 calendar days	24 hours	LMS provider; email; internet
Marking and feedback by Course Assessors	3 calendar days	24 hours	LMS provider; assessor availability
IQA sampling and standardisation	14 calendar days	48 hours	LMS; IQA availability
Certification claims to the Awarding Organisation	7 calendar days	48 hours	AO portal; internet
Safeguarding referral channel	Same working day	Immediate	Email; phone; internet
Finance: receipts, payments, invoicing	7 calendar days	24 hours	Finance software; banking
Learner enquiries and admissions	2 calendar days	24 hours	Email; website; phone

6. Threats and Disruptions

TTT's continuity planning addresses the following categories of disruption, assessed at least annually.

- Technology disruption: LMS outage, email compromise, ransomware, data loss, cloud provider failure
- People disruption: prolonged illness of a key staff member, sudden departure, safeguarding or misconduct case, pandemic
- Supplier disruption: Awarding Organisation portal outage, finance software failure, internet provider failure
- Premises or utilities: power or internet loss at operating locations
- External events: severe weather, public disorder, national emergency
- Regulatory disruption: change or removal of recognition by an Awarding Organisation or Ofqual
- Financial disruption: significant cashflow event, loss of a major reseller or sponsor

7. Prevention and Resilience

TTT reduces the likelihood and impact of disruption through:

- Using reputable cloud services with their own redundancy, for LMS, email and file storage
- Enforcing multi-factor authentication and the controls in the Information Security and Cyber Security Policy
- Maintaining full documentation of operations so continuity does not depend on a single person
- Cross-training staff on core systems where role separation allows
- Keeping a roster of approved associate Course Tutors, Assessors and IQAs for surge or cover
- Maintaining offline copies of key contacts, policies and regulator references for the first 24 hours of a major outage
- Reviewing supplier SLAs and breach clauses annually
- Financial prudence: maintaining a reasonable reserve and up-to-date insurance

8. Incident Command

Role	Responsibility During Incident
Incident Command Contact (Centre Manager, Phenil Mehta)	Declares invocation; leads response; authorises spend and external help; approves communications.
Deputy (Shaily Mehta)	Takes the command role where the Centre Manager is unavailable or conflicted.
Course Coordinator	Coordinates learner communication; tracks actions; logs the incident timeline.

Role	Responsibility During Incident
Course Tutors, Assessors, IQAs	Flex activity under direction; prioritise safeguarding and active cohort continuity.
Critical suppliers	Provide status updates and ETA for restoration; respond to escalation calls.

9. Response Procedure

1. Detect and report: any staff member or associate noticing a significant disruption reports it immediately to the Centre Manager by phone, with email follow-up.
2. Assess and invoke: the Centre Manager (or Deputy) assesses scope and impact and decides whether to invoke this policy as an incident.
3. Contain and stabilise: immediate actions to prevent further harm, including isolating systems, activating cover staff and contacting suppliers.
4. Communicate: use the communications protocol in Section 10 to update learners, staff, Awarding Organisations and suppliers.
5. Deliver alternative arrangements: to meet RTO and RPO, including standby suppliers, manual workarounds or revised deadlines for affected learners.
6. Stand down: once critical activities are restored and stable, the Centre Manager formally stands the incident down and notifies those communicated earlier.
7. Review: a post-incident review identifies root cause, what worked, what did not and actions to strengthen the plan.

10. Communications During an Incident

- Learners: prioritised communication by email (and LMS banner where possible), with clear statements of what has happened, what TTT is doing, impact on their course and the next update time
- Staff and associates: rapid communication through email and, where the outage affects email itself, through a prearranged alternative (for example, SMS or a nominated personal number)
- Awarding Organisations: notified where the incident materially affects assessment, certification or a cohort
- Suppliers: escalation to agreed contacts; SLA breaches logged for later review
- Regulators and Police: contacted where the incident involves personal data breach (ICO), criminal activity or a credible threat
- Public statement: where a major incident attracts public attention, a single, approved statement from the Centre Manager is issued; individual staff do not speak to media on TTT's behalf

11. Data, Cyber and LMS Disaster Recovery

- TTT relies on the supplier-side redundancy of cloud services for the LMS, email and file storage; supplier restoration SLAs are recorded in the supplier register
- Where a cyber incident occurs, the Information Security and Cyber Security Policy is activated; the Police and Action Fraud are notified where required
- Where a personal data breach is implicated, the 24-hour internal and 72-hour ICO clock in the Data Protection and GDPR Policy applies
- Where LMS data is at risk, the LMS-migration protections in the Course Terms and Conditions apply: learners retain their own backups and TTT does not charge for work repetition caused by TTT-led migration

12. Learner Protection During a Disruption

- Extensions to submission deadlines are granted proportionately and at no cost to the learner when TTT's service is disrupted beyond the learner's control
- Where an Awarding Organisation withdraws recognition or portfolio submission is delayed, TTT works with the Awarding Organisation to protect valid learner work and, where necessary, arranges transfer to an alternative centre or qualification
- Learners are kept informed of the impact on their expected certification date

13. Testing and Rehearsal

- TTT conducts an annual tabletop exercise covering at least one realistic scenario (for example, LMS outage or compromised email)
- Critical backups and access paths (including offline contact lists) are tested annually
- Findings from exercises are logged, actions tracked to closure and the policy updated

14. Financial Resilience and Insurance

- TTT maintains a reasonable cash reserve proportionate to its fixed costs and contingent on risk appetite
- TTT holds Professional Indemnity, Public Liability, Employer's Liability (where an employee is engaged) and Cyber Liability insurance where proportionate to the risks; policies are reviewed annually
- Insurance documents are held in the Single Central Record and in an offline form accessible during a severe outage

15. Records and Retention

- Incident logs, post-incident reviews, rehearsal records and supplier restoration evidence are retained for 6 years under the Data Retention and Disposal Policy
- Personal data involved in an incident is handled under the Data Protection and GDPR Policy

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, a failed rehearsal, a supplier change, a major change to TTT's operating model or new regulatory expectation. All outcomes are recorded in the Version History at Section 18.

17. Related Documents

This policy should be read alongside:

- Information Security and Cyber Security Policy
- Data Protection and GDPR Policy
- Privacy Notice
- Data Retention and Disposal Policy
- Health and Safety Policy
- Safeguarding and Prevent Duty Policy
- Staff Code of Conduct
- Staff Induction Policy
- Complaints Policy
- Appeals Policy
- Course Terms and Conditions

18. Version History

Version	Date	Author	Summary of Changes
1.0	22/04/2026	Phenil Mehta	A new standalone policy identifying critical activities with RTO and RPO targets, threat categories, prevention controls, incident command structure with named Deputy, response procedure, communications protocol, learner protection during disruption, annual testing and financial resilience. Aligned with ISO 22301 principles scaled to a small online centre.

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**