LONDON ACADEMY FOR APPLIED TECHNOLOGY

LAAT

Business Continuity and IT Disaster Recovery Policy

Institutional Policy

Prepared by: Himanshu, IT Manager / Committee Officer

CONFIDENTIAL – INTERNAL USE ONLY

Field	Detail
Document Title	Business Continuity and IT Disaster Recovery Policy
Document Reference	LAATITPOL-BCDR-001
Department/ Function	Governance, Compliance & Information Management
Oversight Committee	SMT/ Audit, Risk & Finance Committee
Approving Body	Academic Board (recommendation) / Board of Governors (final approval)
Version	V1
Approved Date	24 June 2026
Next Review	Annually from the approval Date
Supersede	None

1. Purpose

This policy establishes the framework for maintaining continuity of critical institutional operations and IT services in the event of a significant disruption, disaster, or emergency affecting the London Academy for Applied Technology (LAAT).

The policy ensures that LAAT can respond effectively to incidents that threaten the delivery of teaching, learning, assessment, student services, and administrative operations across all campuses. It sets out the governance structure, roles, responsibilities, and procedures for business continuity planning and IT disaster recovery.

This policy supports LAAT's obligations under the Office for Students (OfS) regulatory framework, particularly Condition E2 (management and governance), Condition C3 (student protection), and Condition B1 (quality of academic experience), as well as compliance with UK GDPR regarding the protection and availability of personal data.

2. Scope

This policy applies to all LAAT campuses (Tower Hill, Brentford, and Croydon), all institutional IT systems and digital infrastructure, all academic and administrative operations, and all staff, students, and third-party service providers.

2.1 Systems and Services in Scope

The following systems and services fall within the scope of this policy:

- Microsoft 365 tenancy (Exchange Online, SharePoint Online, Microsoft Teams, Entra ID, OneDrive for Business)
- Moodle Virtual Learning Environment (VLE) and associated plugins
- Turnitin (plagiarism detection and assessment submission)
- SEAtS Attendance (student attendance and engagement monitoring)
- Student CRM and admissions systems (SharePoint-based and Power Apps)
- Microsoft Intune (endpoint management and device compliance)
- Microsoft Defender for Endpoint (endpoint detection and response)
- Campus networking infrastructure (switches, access points, firewalls)
- Telephony (RingCentral)
- CCTV and physical access control systems
- Printing infrastructure and shared devices
- Third-party hosted platforms processing student or staff data

2.2 Out of Scope

Personal devices owned by staff or students that are not enrolled in Microsoft Intune are outside the scope of this policy unless they access institutional data through managed applications.

3. Regulatory and Legal Alignment

This policy is aligned with the following regulatory and legal frameworks:

Framework	Relevance
OfS Condition E2	Management and governance — the institution must have adequate arrangements to manage its affairs and deliver its functions effectively
OfS Condition C3	Student protection — the institution must have plans to protect students in the event of material change or closure
OfS Condition B1	Quality of academic experience — continuity of teaching, learning, and assessment
UK GDPR (Article 32)	Security of processing — the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
Data Protection Act 2018	Data controller obligations regarding data integrity and availability
Cyber Essentials / NCSC Guidance	National Cyber Security Centre guidance for higher education on incident response and recovery

Framework	Relevance
LAAT Risk Management Framework	Institutional risk register, RAG rating framework, and escalation procedures

4. Definitions

Term	Definition
Business Continuity	The capability of an organisation to continue the delivery of its critical functions at an acceptable predefined level following a disruptive incident
Disaster Recovery (DR)	The process, policies, and procedures related to preparing for the recovery or continuation of technology infrastructure and systems following a natural or human-induced disaster
Recovery Time Objective (RTO)	The maximum acceptable length of time that a system, application, or function can be offline after a failure or disaster before the impact becomes unacceptable
Recovery Point Objective (RPO)	The maximum acceptable amount of data loss measured in time — the point in time to which data must be recovered after an outage
Critical System	Any system whose unavailability for more than 4 hours would materially impact teaching, learning, assessment, student welfare, or regulatory compliance
Major Incident	An event that causes or has the potential to cause significant disruption to one or more critical systems or institutional operations
Business Impact Analysis (BIA)	A systematic process to determine and evaluate the potential effects of an interruption to critical business operations

5. Governance and Responsibilities

Business continuity and IT disaster recovery governance sits within LAAT's existing committee and management structure. The following roles carry specific responsibilities under this policy.

Role	Name	Responsibility
CFOO / Operations Director	Raghav Malhotra	Overall accountability for business continuity. Authorises invocation of the BC plan. Liaison with Governing Body and external regulators.
IT Manager	Himanshu	Operational lead for IT disaster recovery. Maintains DR runbooks.

Role	Name	Responsibility
		Leads technical recovery operations. Reports to CFOO and Risk Panel.
Data Protection Officer (Interim)	Manoj Pongubati	Assesses data protection implications of incidents. Manages ICO notification where required. Advises on GDPR compliance during recovery.
VLE / Moodle Lead & IT Support Officer	Bijay Shrestha	Recovery of Moodle VLE and associated learning platforms. Coordinates with hosting provider on VLE restoration.
Governance Officer	Agrima Shankar	Ensures governance documentation is maintained. Coordinates communication to Governing Body. Maintains BC policy review schedule.
Campus Leads	As designated	Local coordination of campus-level response. Staff and student communication. Facilities and physical access management.
All Staff	All LAAT staff	Awareness of BC procedures. Compliance with incident reporting. Participation in testing and exercises.

5.1 Reporting and Escalation

Business continuity incidents are reported through the institutional incident management process and escalated as follows:

- IT incidents are reported to itsupport@laat.ac.uk or directly to the IT Manager
- The IT Manager assesses severity and invokes the appropriate response level
- Major incidents are escalated to the CFOO / Operations Director within 1 hour
- Data breaches involving personal data are reported to the DPO immediately and to the ICO within 72 hours where required
- The Risk Assessment & IT Monthly Panel receives a standing report on all BC/DR incidents, testing outcomes, and risk status

6. Business Impact Analysis and System Classification

All institutional systems are classified according to their criticality to teaching, learning, assessment, student welfare, and regulatory compliance. The classification determines the recovery priority, RTO, and RPO for each system.

6.1 System Classification

System	Classification	RTO	RPO
Microsoft 365 (Exchange, Teams, Entra ID)	Critical	4 hours	1 hour
SharePoint Online (student records, CRM, governance docs)	Critical	4 hours	1 hour
Moodle VLE	Critical	4 hours	4 hours
Turnitin	Critical	8 hours	24 hours
SEAtS Attendance	High	8 hours	4 hours
Microsoft Intune (endpoint management)	High	8 hours	24 hours
Microsoft Defender for Endpoint	High	4 hours	N/A
Campus Wi-Fi and networking	Critical	2 hours	N/A
RingCentral telephony	High	8 hours	N/A
Student CRM / Power Apps	High	12 hours	4 hours
CCTV and access control	Medium	24 hours	N/A
Printing infrastructure	Low	48 hours	N/A

6.2 Classification Definitions

- Critical: Unavailability for more than 4 hours would materially impact teaching, learning, assessment, or student welfare. Recovery is the highest priority.
- High: Unavailability for more than 8 hours would cause significant operational disruption. Recovery is prioritised after critical systems.
- Medium: Unavailability for up to 24 hours is tolerable with workarounds in place.
- Low: Unavailability for up to 48 hours has minimal impact on core operations.

7. IT Disaster Recovery Procedures

This section sets out the procedures for responding to and recovering from IT incidents affecting critical and high-priority systems.

7.1 Incident Response Levels

Level	Description	Response
Level 1 — Minor	Single system or service degraded. No impact on teaching or assessment. Fewer than 50 users affected.	IT team resolves within normal working hours. Logged on IT support system. No escalation required.
Level 2 — Significant	Single critical system unavailable or multiple non-critical systems affected. Impact on teaching or operations for one campus.	IT Manager coordinates response. CFOO notified within 2 hours. Workarounds deployed. Incident logged on risk register.
Level 3 — Major	Multiple critical systems unavailable. Impact across two or more campuses. Assessment or student data at risk.	CFOO invokes BC plan. IT Manager leads technical recovery. DPO notified if personal data involved. Governing Body informed within 24 hours.
Level 4 — Catastrophic	Total loss of IT infrastructure. Campus inaccessible. Data loss confirmed or suspected.	Full BC plan activation. CFOO leads institutional response. External support engaged. OfS and ICO notified as required. Governing Body emergency meeting convened.

7.2 Recovery Procedures by System Category

Detailed recovery runbooks are maintained separately by the IT Manager and stored on the designated SharePoint site. The following summarises the recovery approach for each system category.

Microsoft 365 and Entra ID

- Microsoft 365 services are cloud-hosted with Microsoft's built-in geo-redundancy and SLA (99.9% uptime)
- Entra ID conditional access policies, security configurations, and group memberships are documented and version-controlled
- Exchange Online mailbox data is protected by Microsoft's native retention policies and litigation hold where configured
- SharePoint Online document libraries are protected by versioning and recycle bin retention (93 days)
- In the event of account compromise, the IT Manager executes the compromised account playbook (password reset, session revocation, MFA re-registration, Defender investigation)

Moodle VLE

- Moodle is externally hosted with the hosting provider responsible for server-level backups
- Course content backups are taken by the VLE Lead on a scheduled basis and stored on SharePoint
- In the event of VLE failure, the hosting provider is contacted immediately and the IT Manager coordinates with the VLE Lead on restoration

- If prolonged outage occurs during assessment periods, the Programme Lead and Quality function are notified to invoke academic continuity arrangements (alternative submission methods, deadline extensions)

Campus Networking and Wi-Fi

- Campus network equipment configurations are documented and backed up
- Spare switches and access points are held at Tower Hill for rapid replacement
- ISP failover arrangements are documented per campus
- If a campus loses connectivity for more than 2 hours during teaching hours, sessions are moved to Microsoft Teams (virtual delivery) and students and staff are notified via email and SMS

Endpoint Devices

- All institutional devices are enrolled in Microsoft Intune with compliance policies enforced
- Device configurations are stored in Intune and can be redeployed to replacement hardware
- Autopilot profiles are maintained for rapid provisioning of replacement laptops and desktops
- A pool of spare devices is maintained at Tower Hill for emergency deployment

8. Business Continuity — Academic and Operational

IT disaster recovery is one component of LAAT's broader business continuity arrangements. This section addresses continuity of academic delivery and operational functions during a disruptive event.

8.1 Academic Continuity

- If a campus becomes inaccessible, teaching sessions are moved to Microsoft Teams virtual delivery within 2 hours where possible
- If Moodle is unavailable during an assessment window, the Programme Lead coordinates with the validating university (Plymouth Marjon University) to agree alternative submission arrangements or deadline extensions
- If Turnitin is unavailable, submissions are accepted via email or SharePoint with manual plagiarism checks until the service is restored
- Student communications are issued via Microsoft 365 (email and Teams). If email is unavailable, the institution's SMS notification service is used
- The Student Protection Plan (required under OfS Condition C3) is invoked if disruption is expected to last more than 5 working days or affects the ability to deliver validated programmes

8.2 Operational Continuity

- Staff are equipped with Microsoft 365 access on personal and institutional devices, enabling remote working if a campus is inaccessible
- Critical governance documents, policies, and records are stored on SharePoint Online and are accessible from any location with an internet connection
- Payroll processing is managed through an external provider with its own continuity arrangements; the Finance function maintains offline payroll data as a contingency

- Physical post and deliveries are redirected to Tower Hill (primary campus) in the event of a campus closure.

8.3 Communication Plan

The following communication channels are used during a business continuity event:

Audience	Primary Channel	Fallback Channel
Staff	Microsoft Teams / Email	SMS notification / Personal mobile
Students	Email / Moodle announcement	SMS notification / Social media
Governing Body	Email / Teams	Telephone
Plymouth Marjon University	Email / Formal letter	Telephone
OfS / Regulators	Formal written communication	Telephone
ICO (data breach)	Online notification portal	Telephone helpline

9. Data Backup and Recovery

Data backup and recovery arrangements are fundamental to IT disaster recovery. The following sets out the backup strategy for institutional data.

9.1 Backup Strategy

Data Category	Backup Method	Frequency	Retention
Microsoft 365 (Exchange, SharePoint, OneDrive)	Microsoft native retention + versioning	Continuous	93 days (recycle bin) + retention policies as configured
Entra ID configuration	Documented configuration export	Monthly	12 months
Moodle VLE content	Hosting provider server backups + manual course backups	Daily (provider) / Weekly (manual)	Provider SLA + 12 months (manual)
Intune device configurations	Intune cloud-stored profiles	Continuous	As long as profile exists
Network equipment configs	Manual configuration export	After each change	12 months
Student records (SharePoint)	SharePoint versioning + retention policies	Continuous	Duration of study + 6 years
CCTV footage	Local NVR storage	Continuous	30 days (standard)

9.2 Backup Testing

Backup restoration is tested at least annually for each critical and high-priority system. Test results are recorded and reported to the Risk Assessment & IT Monthly Panel. Any backup failure or gap identified during testing is logged on the risk register and remediated within the timescales agreed at the panel.

10. Testing and Exercising

The business continuity and IT disaster recovery arrangements set out in this policy must be tested regularly to ensure they remain effective and that staff are familiar with their roles.

Test Type	Frequency	Scope
DR runbook walkthrough	Annually	IT Manager reviews and updates all DR runbooks with the IT team
Backup restoration test	Annually	Restore test for each critical system to verify data integrity and RTO/RPO compliance
Tabletop exercise	Annually	Scenario-based discussion exercise involving IT, Operations, Academic, and Quality leads
Communication test	Annually	Test of staff and student notification channels (email, SMS, Teams)
Full simulation	Every 2 years	End-to-end simulated incident involving invocation of the BC plan and DR procedures

Test results, lessons learned, and resulting actions are reported to the Risk Assessment & IT Monthly Panel and recorded on the institutional risk register.

11. Third-Party and Supplier Continuity

LAAT relies on a number of third-party suppliers and cloud service providers for critical systems. The following requirements apply to all suppliers whose services are classified as critical or high under this policy:

- Suppliers must provide evidence of their own business continuity and disaster recovery arrangements upon request
- Service level agreements (SLAs) must include uptime commitments, incident response timescales, and data recovery capabilities
- The IT Manager maintains a register of critical suppliers and their SLA terms

- Supplier BC/DR arrangements are reviewed annually as part of the contract management process
- Where a supplier is unable to meet LAAT's RTO/RPO requirements, this is logged as a risk on the institutional risk register and reported to the Risk Panel

12. Cyber Security Incident Integration

Cyber security incidents (ransomware, data breach, account compromise, denial of service) are managed under this policy's incident response framework with additional obligations:

- The IT Manager leads the technical response using Microsoft Defender for Endpoint, Entra ID sign-in logs, and Exchange Online audit logs
- The DPO is notified immediately where personal data may be compromised
- ICO notification is made within 72 hours where the breach is likely to result in a risk to the rights and freedoms of individuals
- Affected individuals are notified without undue delay where the breach is likely to result in a high risk to their rights and freedoms
- A post-incident review is conducted within 10 working days and findings are reported to the Risk Assessment & IT Monthly Panel
- NCSC reporting is considered for incidents meeting the threshold for significant cyber-attacks on the education sector

13. Student Protection

In accordance with OfS Condition C3, LAAT maintains a Student Protection Plan which is invoked where a business continuity event may affect the institution's ability to deliver validated programmes or provide the academic experience students are entitled to expect.

The Student Protection Plan covers scenarios including but not limited to:

- Prolonged campus closure (more than 5 working days)
- Sustained loss of VLE or assessment platform during a submission or examination period
- Loss of student records or assessment data
- Material change to programme delivery arrangements

Where a business continuity event triggers the Student Protection Plan, the CFOO / Operations Director is responsible for liaison with Plymouth Marjon University (the validating partner) and the OfS as required.

14. Review and Maintenance

This policy is reviewed annually by the IT Manager and approved by the CFOO / Operations Director. The review considers:

- Changes to institutional IT infrastructure or systems
- Changes to the regulatory environment (OfS, UK GDPR, Cyber Essentials)

- Lessons learned from incidents, near-misses, and testing exercises
- Changes to third-party supplier arrangements
- Feedback from the Risk Assessment & IT Monthly Panel

The policy is also reviewed following any major incident or significant change to LAAT's IT estate. All changes are recorded in the document control section below.

15. Document Control

Field	Detail
Document Title	Business Continuity and IT Disaster Recovery Policy
Document Reference	LAATITPOL-BCDR-001
Version	1.0
Date	June 2026
Author	Himanshu, IT Manager
Approved By	Raghav Malhotra, CFOO / Operations Director
Panel Chair	Manoj Pongubati (Interim)
Next Review	June 2027
Storage Location	LAAT OFS Internal Audit / Himanshu – IT Policies
Classification	Internal — Governance

15.1 Version History

Version	Date	Author	Changes
1.0	June 2026	Himanshu, IT Manager	Initial version

Any queries regarding this policy should be directed to: Himanshu (IT Manager) via itsupport@laat.ac.uk.