Business Continuity Plan

Gtec Media Limited
Policy Owner: Gtec Media Limited
Approved By: Geoff Hunter, Director
Version: 1.0
Effective Date: 21st January 2026
Review Date: Annually

1. Purpose

The purpose of this Business Continuity Plan (BCP) is to ensure that Gtec Media Limited can continue to deliver critical business operations and minimise disruption in the event of an incident, emergency, system failure, cyber incident, utility outage, severe weather event, staff absence, or any other disruption affecting normal operations.

This plan sets out the organisation's approach to maintaining continuity of services, protecting learners, clients, staff, contractors, systems, and business data, and restoring operations within acceptable timescales.

2. Scope

This Business Continuity Plan applies across all areas of Gtec Media Limited's operations including:

- Adult Skills and Learning provision
- Tutor-led online learning delivery
- Digital inclusion and media literacy programmes
- IT support and technical services
- Website support and maintenance
- Digital marketing services
- Research and consultancy activities
- Remote working operations
- Office-based activities
- Contractor and associate activities undertaken on behalf of the organisation

This policy applies to:

- Employees
- Directors
- Freelancers and associates
- Tutors and trainers
- Contractors
- Learners
- Clients and stakeholders

3. Objectives

The objectives of this plan are to:

- Protect the health, safety and welfare of staff, learners and stakeholders
- Ensure continuity of critical business functions
- Minimise disruption to learning delivery and client services
- Protect organisational data and IT systems
- Maintain communication with learners, staff and clients
- Restore normal operations as quickly as possible
- Ensure compliance with contractual, legal and regulatory obligations
- Reduce financial and reputational damage

4. Key Business Activities

Critical activities covered by this plan include:

Business Function	Priority Level
Online learning delivery	Critical
Learner communication and support	Critical
IT support services	Critical
Email and communications systems	Critical
Website hosting and maintenance	High
Digital marketing campaigns	Medium
Research and consultancy services	Medium
Administration and finance	High

5. Potential Business Disruptions

Potential disruptions may include:

- Cyber attack or malware infection
- Internet outage
- Website/server failure
- Cloud service disruption
- Loss of access to business premises
- Severe weather
- Fire or flood
- Illness or absence of key personnel
- Data breach
- Power failure
- Hardware failure
- Telecommunications failure
- Pandemic or public health emergency
- Third-party supplier disruption

6. Roles and Responsibilities

Director

The Director is responsible for:

- Overall implementation of the Business Continuity Plan
- Coordinating incident response
- Communicating with clients, learners and stakeholders
- Making operational decisions during incidents
- Reviewing lessons learned following disruption

Staff, Tutors and Contractors

All staff, tutors and contractors are responsible for:

- Following business continuity procedures
- Reporting incidents promptly
- Protecting company information and systems
- Maintaining secure remote working practices
- Supporting continuity arrangements where required

7. Business Continuity Measures

Remote Working Capability

The organisation maintains the ability to operate remotely using:

- Cloud-based systems
- Video conferencing platforms

- Remote communication tools
- Remote access to business systems
- Secure password-protected devices

This enables continuation of:

- Online learning delivery
- Learner support
- IT support services
- Digital marketing operations
- Administrative activities

Data Backup and Recovery

Gtec Media Limited maintains:

- Regular automated backups of critical business data
- Cloud-based storage solutions
- Password-protected systems and accounts
- Secure hosting environments
- Malware protection and firewall systems
- System update and patch management procedures

Backups are tested periodically to ensure recovery capability.

Cyber Security and IT Resilience

The organisation implements reasonable technical controls including:

- Antivirus and malware protection
- Strong password requirements
- Multi-factor authentication where available
- Secure remote access
- Website and server monitoring
- Software update management
- Access control procedures

Any cyber incident will be managed in line with the organisation's Data Protection and Information Security procedures.

8. Communication During Disruption

In the event of disruption, communication may be made through:

- Email
- Telephone
- Video conferencing

- Website announcements
- Messaging platforms

Affected learners, clients and stakeholders will be informed as soon as reasonably practicable regarding:

- Nature of the disruption
- Expected impact
- Alternative arrangements
- Estimated restoration times

9. Alternative Delivery Arrangements

Where face-to-face delivery becomes unavailable, the organisation may:

- Switch to remote online delivery
- Reschedule sessions
- Provide recorded learning materials
- Offer alternative communication methods
- Adjust delivery times where appropriate

The organisation will seek to minimise interruption to learner participation and client services wherever possible.

10. Incident Response Procedure

In the event of a significant disruption:

Step 1 – Identify the Incident

Assess:

- Nature of disruption
- Services affected
- Risks to learners, staff or clients
- Estimated duration

Step 2 – Activate the Plan

The Director will determine whether to activate business continuity procedures.

Step 3 – Implement Immediate Controls

Examples:

- Move to remote working
- Restore systems from backup

- Contact suppliers
- Suspend affected services temporarily
- Redirect communications

Step 4 – Communicate

Notify affected stakeholders as appropriate.

Step 5 – Restore Operations

Prioritise restoration of critical services.

Step 6 – Review

Following recovery:

- Review effectiveness of response
- Identify lessons learned
- Update procedures if necessary

11. Third-Party Suppliers

The organisation relies on third-party providers for certain services including:

- Hosting providers
- Internet providers
- Cloud platforms
- Video conferencing systems
- Software providers

Where possible:

- Reputable providers are used
- Backup solutions are maintained
- Alternative providers may be considered where appropriate

12. Testing and Review

This Business Continuity Plan will be:

- Reviewed annually
- Reviewed following significant incidents
- Updated following operational or technological changes
- Tested periodically through scenario-based reviews where appropriate

13. Related Policies

This plan should be read alongside:

- Health and Safety Policy
- Data Protection Policy
- Information Security Policy
- Cyber Security Procedures
- Complaints and Compliments Policy
- Safeguarding Policy
- Equality and Diversity Policy

14. Approval

This Business Continuity Plan has been approved by Gtec Media Limited and applies across all organisational operations.