



Address: 2 Lord Street, Oldham OL1 3EY

©2024 NxtGen Education

Policy Name	Business Continuity Plan (BCP)
--------------------	--------------------------------

Recent Review Date	December 2024	Next Review Date	December 2025
---------------------------	---------------	-------------------------	---------------

1. Purpose of the Plan

The purpose of this Business Continuity Plan (BCP) is to ensure that NXT GEN Education (“NXT GEN”) can:

- Continue providing essential services and training delivery during disruptions
- Protect learners, staff, data, and physical assets
- Maintain compliance with awarding body and regulatory requirements (e.g., Ofqual)
- Resume full operations as quickly and safely as possible following an incident

This plan applies to all NXT GEN campuses, teaching locations, online learning environments, systems, staff, and learners.

2. Scope

The BCP covers disruptions including (but not limited to):

- Loss of premises or facilities
- IT system failure or cyberattack
- Loss of internet or communication systems
- Staff shortages
- Illness outbreaks or public health emergencies
- Loss of awarding body approval
- Loss of key suppliers or partners
- Data breaches
- Natural disaster, fire, or flooding
- Major safeguarding incidents

3. Objectives

NXT GEN will:

- Minimise operational disruption
- Protect learners and uphold their right to complete their qualifications
- Ensure assessments, results, and certification continue wherever possible
- Maintain clear communication with all stakeholders
- Protect NXT GEN’s reputation and regulatory status
- Meet obligations to awarding bodies (e.g., TQUK), Ofqual and other regulators
- Ensure coordinated response and clear lines of responsibility

4. Responsibilities

4.1 Management Team

- Lead overall response during an incident
- Approve activation of the Business Continuity Plan
- Liaise with awarding bodies, regulators, insurance providers, and emergency services

- Authorise temporary relocation, alternative delivery methods, or temporary suspension of services
- Coordinate the business continuity response
- Monitor risk and maintain the BCP
- Liaise with partners, centres, and suppliers
- Maintain a log of incidents and actions
- Notify awarding bodies of any event with potential to cause an Adverse Effect

4.2 IT & Data Management Team

- Maintain system backups and cybersecurity protections
- Restore IT infrastructure when required
- Support remote delivery if on-site learning is disrupted

4.3 All Staff

- Follow BCP instructions during incidents
- Know evacuation procedures
- Report concerns or disruptions promptly
- Maintain continuity of teaching, assessment, and learner support where possible

4.4 Partners and Delivery Sites

All partner centres must comply with:

- NXT GEN continuity expectations
- Data protection requirements
- Awarding body requirements

5. Risk Assessment and Mitigation Strategies

Below is a summary of the key risks and mitigation approaches.

5.1 Loss of Premises (fire, flood, forced closure, lease termination)

Impact: Disruption to training delivery, records access, administration

Mitigation:

- Multiple delivery sites where possible
- Capability for remote/online delivery
- Cloud-based storage of learner records
- Contact arrangements with alternative local venues
- Insurance coverage

Continuity Actions:

- Activate remote learning via online platforms
- Relocate to alternative venue
- Inform learners and staff within 24 hours
- Notify awarding bodies and regulators if required

5.2 Loss of Staff or High Levels of Absence

Impact: Inability to deliver teaching, assess learners, or administer services

Mitigation:

- Maintain a list of approved assessors/trainers
- Cross-training staff across essential functions
- Remote teaching capabilities

Continuity Actions:

- Redeploy staff temporarily
- Use qualified subcontractors or partner trainers
- Prioritise essential activities (assessments, safeguarding, certification)

5.3 Loss of IT Systems or Cyber Attack

Impact: Data loss, inability to deliver online learning, communication failures

Mitigation:

- Regular system backups
- Cloud-based platforms with redundancy
- Antivirus protection, firewalls, password policies
- Staff training in cyber security

Continuity Actions:

- Switch to backup servers or alternative platforms
- Reset compromised accounts
- Inform affected users
- Report breaches to ICO within legal deadlines where required

5.4 Loss of Awarding Body Approval

Impact: Inability to deliver regulated qualifications

Mitigation:

- Maintain full compliance with awarding bodies
- Internal audits and quality assurance
- Keep alternative awarding body relationships active

Continuity Actions:

- Transfer learners to an approved alternative centre
- Work with awarding bodies to protect learner outcomes
- Communicate plan clearly to learners and partners

5.5 Public Health Emergency (e.g., pandemic)

Impact: Restricted access to premises, reduced staff capacity

Mitigation:

- Remote learning capability
- Health and safety risk assessments
- Infection control measures

Continuity Actions:

- Switch to online delivery
- Extend deadlines or modify assessments where permitted
- Communicate safeguarding and mental health support options

5.6 Loss of Key Suppliers or Partners

Impact: Disruption to teaching spaces, exam invigilation, equipment access

Mitigation:

- Maintain multiple supplier options
- Formal agreements with backup partners

Continuity Actions:

- Change supplier where required
- Notify awarding bodies if any change affects qualification delivery

6. Continuity Procedures

6.1 Activation of the Plan

The BCP will be activated when:

- An incident significantly disrupts operations
- There is a threat to learner safety or completion of qualification
- A regulator or awarding body requires immediate action
- Activation must be approved by the Managing Director or a designated senior leader.

7. Communication Protocol

Internal Stakeholders

- Email/text alerts to staff
- Emergency staff briefing (in-person or remote)
- Daily updates as required

Learners

- Call/SMS/email notifications
- Updates via Moodle/VLE, website, or social media

Awarding Bodies

NXT GEN will notify awarding bodies of:

- Changes to delivery
- Disrupted assessments
- Safeguarding concerns
- Any incident with potential to cause an Adverse Effect

External Bodies

Where appropriate, NXT GEN will liaise with:

- Landlords / building management
- Emergency services
- Insurance providers
- The ICO (in case of data breach)

8. Protecting Learners

NXT GEN is committed to safeguarding learners' rights to complete their programme. In the event of disruption:

- Learners will be offered alternative delivery options
- Extensions or assessment adjustments may be requested through awarding bodies
- Transfers to alternative centres will be arranged if necessary
- Learner records will remain accessible to support continuity

9. Backup and Recovery

Data Backup

- Daily automated backups to secure cloud storage
- Backups tested monthly

Systems Recovery

- Critical systems targeted for recovery within 24 hours
- Staff issued alternative login details if systems are compromised

10. Review and Testing

This plan will be:

- Reviewed annually
- Tested at least once per year (tabletop exercise or simulation)
- Updated after incidents or organisational changes

11. Plan Storage and Access

Copies of this plan will be:

- Stored securely online (SharePoint/OneDrive)
- Available to Management Team and key departmental leads
- Accessible on Website

Appendices (available on request)

Appendix A – Risk Register

Appendix B – Emergency Contact List

Appendix C – Incident Log Template

Appendix D – Communication Templates

Appendix E – Alternative Delivery Location List

Appendix F – Cyber Incident Response Procedure