Business Continuity & Disaster Recovery Plan

1. Purpose
This plan explains how JC Training & Consultancy Ltd responds to, manages and recovers from any disruption that affects the delivery of training, assessment, safeguarding, staffing, systems or operational activity.
Its purpose is to ensure that learners are safeguarded, learning continues where possible, critical services are prioritised, and normal operations are restored in a safe and controlled way.
This plan is designed for use during live incidents and clearly sets out actions, responsibilities and escalation routes.

2. What This Plan Covers
This plan applies to any situation that disrupts normal business operations. This includes full or partial disruption.
Examples include loss of IT systems, cyber incidents such as ransomware or data breach, loss of premises due to fire, flood or damage, significant staff absence, safeguarding incidents, severe weather or travel disruption, power or utilities failure, public health emergencies, and regulatory intervention or funding body action.
The plan applies whether disruption affects a single learner, a group of learners, a delivery site, or the entire organisation.

3. Critical Priorities During Any Incident
During any disruption, the organisation follows a strict order of priorities.
The first priority is safeguarding. Any risk to a learner or staff member is escalated immediately and managed under safeguarding procedures.
The second priority is safety of staff and learners, including evacuation, relocation or suspension of activity where required.
The third priority is protection of data and systems to ensure learner records and compliance information are not lost or compromised.

The fourth priority is continuity of learning and assessment activity where it is safe and possible to do so.
The fifth priority is communication with staff, learners, employers and external agencies.
The final priority is recovery and return to normal operations.

4. Roles and Responsibilities During Disruption
The Director is responsible for overall incident control, strategic decisions and external liaison with regulators and funding bodies.
The Operations Lead is responsible for coordinating delivery continuity, staff deployment, learner communication and operational recovery.
The Quality Lead is responsible for ensuring assessment integrity, compliance with awarding bodies and maintenance of evidence.
The Finance Lead is responsible for emergency expenditure, supplier continuity and financial control during disruption.
All staff are responsible for reporting issues immediately, following instructions, and maintaining communication through agreed channels.

5. Immediate Response Procedure (First 0 Hours)
When an incident occurs, the first staff member aware must notify a member of the Senior Leadership Team immediately.
The Senior Leadership Team will assess the situation and confirm the severity level.
If there is any immediate risk to life or safety, emergency services are contacted without delay.
If systems are unavailable, staff revert to mobile communication or pre-agreed backup channels.
A decision is made whether to activate full or partial business continuity procedures.
A central communication message is issued to staff and learners confirming the situation and next steps.
No staff member other than the designated leads communicates externally.

6. Short Term Response (First 8 Hours)
Once the incident is stabilised, the organisation focuses on maintaining essential services.
Learners are informed of any changes to delivery schedules.
Staff are redeployed where needed to support safeguarding, communication or delivery continuity.
If premises are unavailable, remote working arrangements are activated.
If IT systems are unavailable, manual recording processes are used temporarily and stored securely until systems are restored.
Safeguarding checks continue without interruption using alternative contact routes.
The Senior Leadership Team meets regularly to review progress and adjust actions.

7. Continuity of Learning
Where possible, learning continues through remote delivery, rescheduled sessions or alternative platforms.
If learners cannot access normal sessions, staff maintain contact and provide updates, guidance and revised learning plans.
Assessments are paused where required for safety or integrity reasons and resumed once conditions are stable.
All learner progress is recorded manually if systems are unavailable and transferred back into systems once restored.

8. IT Failure or Cyber Incident Response
If systems fail or are compromised, access is immediately restricted to prevent further damage.
The IT lead or external provider is contacted immediately.
All staff switch to offline contingency processes, including paper-based recording and mobile communication.
Safeguarding and learner contact details are accessed through secure backup copies.
No data is deleted or altered until the incident is resolved and authorised recovery is complete.

9. Loss of Premises Response
If a site becomes inaccessible, staff and learners are relocated to an alternative agreed location or moved to remote delivery.
Attendance registers are taken immediately to confirm all learners and staff are safe.
The Operations Lead coordinates relocation and informs learners of temporary arrangements.
Equipment and records are recovered where safe to do so.

10. Staffing Shortage or Loss of Key Staff
If significant staff absence occurs, priority delivery areas are maintained first.
Non-critical activity is paused.
Available staff are redeployed based on competence and safeguarding clearance.
External associates may be used where necessary and appropriate.

11. Communication During Incident
All communication is controlled through the Senior Leadership Team.
Updates are provided to staff and learners at regular intervals.
Messages are factual, clear and avoid speculation.
If information is not yet known, this is clearly stated.
Only approved staff communicate with external bodies, employers or regulators.

12. Data Backup and Recovery
All key systems are backed up regularly and stored securely.
If systems are lost, the most recent backup is restored as soon as possible.
Manual records created during the disruption are reconciled and entered into systems once restored.
Data integrity is checked before systems return to full operation.

13. DFE and Regulatory Engagement
If disruption is severe or prolonged, the organisation informs the DFE where required.
Full cooperation is provided to any regulatory body involvement or intervention.
All learner data, evidence and records are made available to support continuity of provision.

14. Recovery and Return to Normal Operations
Once immediate risks are resolved, focus moves to full recovery.
Systems are restored and tested.
Delivery is gradually reintroduced.
Learners are supported to catch up on missed learning.
Staff return to normal duties.
A review is completed to identify lessons learned and improve future resilience.

15. Review of This Plan
This plan is reviewed annually and after any major incident.
Updates are communicated to all staff.