BUSINESS CONTINUITY POLICY

Policy Group: Health & Safety

Effective: December 2025

Approved: Business Critical Response Team

Responsible Officer: Steve Williams, Head of Risk

Next Renew Date: December 2026

Ref no: 2.4

GUIDANCE

Vision

Transform lives through learning

Values

P

PASSIONATE - We are passionate about inspiring young people, adults and our Purple People to be their best and we take pride in creating a positive learning environment to fulfil their potential.

U

UNSTOPPABLE - We are unstoppable in our quest for the pursuit of excellence. We are dedicated and resilient to develop ourselves and our learners.

R

RIGHT - We treat each other with respect and strive to do the right thing through insight, inclusion, honesty, growth and trustworthiness.

P

PARTNERSHIPS - We support the people surrounding us in our everyday lives, building effective partnerships with businesses, learners and all stakeholders where we can pass on our knowledge and skills to help them meet their goals.

L

LEARNERS - Learners are at the centre of everything we do and we are driven to provide life-changing and life-long learning for them.

E

EMPOWERED - We encourage our Purple People to be independent and autonomous to maximise their goals surpassing their barriers and targets. Feel it, believe it, live it.

Tone of voice

Our tone of voice takes its direct influence from our core values. We are passionate about people and learners and are driven to get the best out of everyone by understanding them. We are caring and supportive, as well as being determined and striving for growth. We talk with purpose and enthusiasm in a way that connects and empowers people.
Innovation is at the heart of Learning Curve Group and we're always thinking about what's next!

SUMMARY CHANGES

Date	Page	Details of Amendments
January 2022	Whole Document	Annual Review
June 2022		Role Changes
December 2022	Whole Document	Annual Review
December 2023	Whole Document	Review and split BCP and Incident/Crisis management to own sections
December 2024	Whole Document	Annual review.
December 2025	Whole Document	Annual review – Legislative updates (DUAA 2025, Martyn's Law, cyber resilience bill), strengthened cyber & data continuity, expanded testing and publication clauses; updated RTOs; clarified roles and emergency file contents

INTRODUCTION

Learning Curve Group (LCG) is one of the largest national training providers in the UK, providing education and training nationally. All companies within the LCG family uphold the same company Vision, Mission and Core Values and follow our group policies and procedures.

This policy sets out the means to provide a flexible response framework so that Learning Curve Group can:

- Respond effectively to a major disruptive occurrence (incident management) across the business.
- React appropriately to changes in key staff that would potentially impact on the success of the business.
- Maintain delivery of critical activities during an incident (business continuity).
  Return to business as usual (resumption and recovery) as soon as feasible after an incident.

Applies to

This policy applies to all our people, premises and functions and should be read in conjunction with our individual departmental/site business continuity plans and emergency procedures and used in conjunction with any property owner or shared site procedures that may also apply.

Reason for policy

This Business Continuity Policy (BCP) details steps that should be taken before, during and after any disruptive occurrence to maintain the delivery of critical services and financial viability of the business. The impact of any serious disturbance may affect the business delivery of education, safety/welfare of colleagues and learners, it may have financial consequences, reputation damage or possible environmental consequences. The main objectives of this policy are:

- To safeguard the safety and welfare of colleagues, learners, and visitors and where applicable the public.
- To resume provision of services (internally and externally) at the earliest opportunity and, where possible, secure a continuation of learning for learners.
- To maintain the identity of the company and limit financial consequences.
- To limit any reputational damage.
- To return to business as normal as soon as possible after the incident and limit the impact on our customers and learners.

LEGISLATIVE & REGULATORY FRAMEWORK (UPDATED DECEMBER 2025)

LCG's BCP is aligned to and will be reviewed against the following UK legislation, regulation and official guidance. Where an act has received Royal Assent but is not yet in force, LCG will prepare during the implementation period.

- Health and Safety at Work etc. Act 1974 (general duties of employers and employees).
- Management of Health and Safety at Work Regulations 1999 (risk assessment; competent persons; emergency procedures).

- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR) – statutory reporting of specified incidents.
- Civil Contingencies Act 2004 and statutory guidance: Emergency Preparedness (Category 1/2 responders' duties incl. BCM, exercising and publication of aspects of plans).
- UK GDPR and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025 (DUAA) – data protection continuity, 72-hour breach reporting, complaints process and recognised legitimate interests; phased commencement from June 2025 to June 2026.
- Terrorism (Protection of Premises) Act 2025 (Martyn's Law) – Royal Assent 3 April 2025; 24-month implementation period; tiered duties for premises/events (standard tier 200–799; enhanced tier 800+); regulator function within SIA.
- Cyber Security and Resilience (Network and Information Systems) Bill (introduced November 2025) – proposed expansion of NIS Regulations scope (managed service providers, data centres, critical suppliers) and stricter incident reporting (initial within 24 hours and follow-up within 72 hours) – LCG will monitor and prepare accordingly.

National Cyber Security Centre (NCSC) resilience and incident management guidance – board accountability, offline/printed response plans, architecting for recovery.

This policy and procedure do not form part of your terms and conditions of employment and can be changed at any time as we deem appropriate.

POLICY

Purpose

To provide guidance and support to enable us to tackle the impact of severe disruptions due to a variety of one-off, but credible, causes. It will co-ordinate the response of all our departments alongside their individual business continuity plans to ensure business critical functions are reinstated as soon as possible, while full restoration of all services is planned and implemented on a concurrent basis.

Circumstances

The policy will be activated in response to an incident causing significant disruption to the business, particularly in delivery of key or critical activities e.g.

- Loss of key staff or skills due to above normal levels of absenteeism e.g., illness (pandemic).
- Loss of critical staff where recruitment and replacement is challenging.
- Total or partial loss of utility provision or critical systems prohibiting delivery of services.
- Denial of access to facilities due to damage or landlord restrictions.
- Loss of a key resource delivering critical support.
- Serious injury or death.
- Release of toxic or harmful materials in the vicinity and possible environmental incident.
- Sub-contractor issues that may affect the contract and learners enrolled where LCG will take over delivery and support fully.
- Area incident prohibiting access (e.g., terrorist attack/local threat level changes) and restricted travel/public transport.

The above list is not exhaustive, and other circumstances may trigger the plan to be activated.

Health & Safety Legislation

Under the Health and Safety at Work etc. Act 1974 and associated regulations (e.g., Management Regs, RIDDOR), continual assessment of risks and prevention of harm during disruptions is required. and this is incorporated into the response by the LCG ERT and H&S Team/HoR.

Operational Resilience (Financial and General Business)

As per the FCA/PRA Operational Resilience Rules required mapping of "important business services" and testing against impact tolerances by 31 March 2025. LCG will continue to identify vital services and assign an impact tolerance and recovery triggers within the overall business risk management

Data Protection & IT Resilience, Cyber Continuity

Under UK GDPR and evolving guidance (Data (Use and Access) Act effective 19 June 2025), it's mandatory to maintain a risk-based BCP and Disaster Recovery Plan that safeguards sensitive or personal data.

Key actions include:

- Off-site backups with frequency appropriate to data sensitivity.
- Regular testing of backup and restore processes.
- Ensuring staff awareness and plan accessibility

LCG will maintain off-site backups for key systems and data, test recovery processes regularly, and ensure staff can access plans during incidents. We will maintain an internal breach response process, including risk triage, containment, decision-making on ICO notification within 72 hours where required, and communication to affected individuals where high risk exists. We will also maintain supply chain assessments and vendor continuity procedures.

Cyber Security & Supply Chain Resilience

The **Cyber Security and Resilience Bill** expand obligations for key sectors and digital infrastructures, including incorporating cyber continuity alongside IT recovery:

- Mandatory supply-chain risk assessments.
- Incident reporting within 24–72 hours.
- Include defined roles and timelines for cyber-incident detection, reporting, and remediation.
- Perform periodic supply chain assessments and vendor continuity checks.

Business Recovery Timescales (RTOs)

In the event of a situation which threatens business continuity, there are deemed to be several business functions which must be maintained or reinstated as a priority. A Recovery Time Objective (RTO) has been assigned to each of these functions as shown below.

Function	Recovery Time Objective (RTO)
Leadership – Business Critical Response Team	2 hours
Safeguarding and Prevent services	2 hours
Health and Safety assessment	1 day
Communication with Stakeholders/Learners/Employers	1 day
IT recovery assessment	1 day
Data protection & cyber incident response (Triage, containment, reporting)	4 hours
Insurance assessment	5 days
Financial transactions	5 days
HR	4 hours
Website/social media	4 hours
E Portfolio	1 day
Continuation of Learning	2 days
Critical supplier/vendor continuity assessment	5 days

Some of the areas listed may be suspended during any disruptive occurrence, however, they must be reinstated as soon as is viable based on the RTO listed here. Any arrangements to adjust staffing levels in different areas will be by negotiation with line managers and authorised by the appropriate member of the Executive Team.

Escalating a serious incident

All serious incidents should be reported to the relevant Executive Director or Head of Risk immediately afterwards of initial response, who will then inform relevant staff to respond. If the disruption has resulted in the loss of access to one of our sites, an Emergency Response Team (ERT) meeting should be held at one of the other company sites nominated by the relevant Executive Director or Head of Risk or designated deputy. Any out of hours incident would, in the first instance, normally be reported via internal monitoring systems to the on-call security response teams.

Responsibility for Plan Activation

A nominated ERT will be activated by the Executive Team ERT Lead or designated deputy in their absence of HoR, as detailed in the Incident Response Policy as soon as possible after the incident. A member of this team will be responsible for standing down on this plan once everything is returned to business as usual. Members of the ERT and any deputies will hold site specific information for property owners, IT managed services and other business critical information that may need to be accessed during any event. This must be always kept secure and checked for any changes on a 6-monthly basis by each Directors responsible for business specific areas and supported by the Head of Risk.

Critical Roles

LCG identifies critical roles in the business that would have a significant impact on the functions of the company should they cease or individual leave the business. These include but are not limited to:

- Executive Directors
- External Clients Services Director
- Heads of Department
- Subcontract Manager
- Bid writers
- Senior Designated Safeguarding Leads and Designated Safeguarding Leads
- Data Protection Officer (DPO)
- IT Security Officer/IT Services Manager

LCG has succession plans and/or identified people who will pick up a critical role should it be required. In line with our values, we endeavour to empower our people and provide every opportunity for training, job shadowing and career progression which is supported by our Purple People (Training) Academy. We believe in growing our own specialists ready to take on the challenge of a new role and continue to create a working culture that successfully promotes personal and professional development.

Military Academies

Within our Military Academies we follow the strict practices of the Ministry of Defence (MOD) whilst using their sites and the incident officer would consult with the MOD, should there be any critical incidents. The military works on the ‘alert state for the whole of the UK (the threat level from Northern

Ireland will remain separate), but threats may be specific to the site and intelligence led information. The levels are:

- Critical – an attack is highly likely in the future.
- Severe – an attack is highly likely.
- Substantial – an attack is likely.
- Moderate – an attack is possible but not likely.
- Low – an attack is highly unlikely.

Each of our military academies have an alert board on entrance and exit of the camp. Academy Managers are briefed and pay attention to the alert state and if there are any changes or if specific intelligence comes in, guidance is sought from the MOD. LCG will work with the Reserve Forces' and Cadets' Associations (RFCA) to support in the re-locating of our learners to a temporary venue, should it be necessary. Other establishments may be used if the threat/incident is deemed long term.

Individual Departmental Business Continuity Plans

Each department must maintain a Disaster Recovery/Continuity plan detailing:
Information sharing during/after incidents to teams and the wider business.
Alternative premises (short/long term) until normal service is resumed.
Key staff responsible for decision-making in their departments.
Service mapping of critical activities, dependencies and single points of failure.

Upon activation of this plan, the Executive Lead or nominated deputy will trigger the ERT.
The primary objective is to manage the situation and minimise harm to colleagues, learners, visitors, buildings, assets, and the public.
Plans are stored in SharePoint, and a hard copy is held by relevant managers should access be compromised. Plans will be updated when changes occur.

Emergency Site File

Any evacuation is dealt with via our internal fire evacuation procedures or on advice from the emergency services/property owner. The emergency file should be stored in the reception/admin office of each site. Members of the ERT will also have site specific information kept in a separate secure location and an online BCP folder which can be accessible when required. The on-site file should contain the following items:

- Emergency telephone numbers
- List of on-site fire wardens
- List of on-site first aiders
- Floor plans for LCG specific areas and associated areas if required.
- Disaster recovery plan
- Current Personal Emergency Evacuation Plans (PEEP) for site staff, learners or clients on site requiring one.
- Run, Hide, Tell Guidance. RUN HIDE TELL | ProtectUK
- Citizen Aid App and printed actions on pages. The citizenAID App is a 'lifesaving' app
- Local terrorism security procedures aligned to Martyn's Law (where applicable)
- Up-to-date contact information for staff and learners (accessible via secure systems)

Any other critical items, e.g., up to date contact information for staff, learners, any other critical parents/carers, will be available via any internet-enabled computer and kept updated by the Chief

People Officer or Director of Funding and MIS. The file should be taken out of the LCG premises by the nearest person, only if it is safe to do so. The emergency file will be checked bi-annually for accuracy of information by the Academy Managers and supported by Health & Safety Team.

Testing the plan

This policy will be assessed annually alongside the Incident Response policy by using the tabletop method and, where appropriate, live-play exercises. Exercises will include cyber scenarios, loss of premises, and safeguarding/terrorism scenarios (where applicable). Lessons learned will be recorded and plans updated. Selected non-sensitive aspects may be published to meet statutory duties and promote preparedness.
This tests the theoretical ability of all areas across Learning Curve Group to respond to a business continuity incident.

It Centres on role-playing and will be done in a training room. The tabletop exercise is a discussion, during which personnel review their ERT-defined roles and discuss their responses during an adverse event simulation. This testing will be conducted annually in line with LCG yearly review of all business continuity and disaster recovery planning.

This has been reviewed and approved by our Executive and Emergency Response Team (ERT).

The BCP Strategy also incorporates risk evaluation in relation to Martyn’s Law (protect Duty Act 2025)

This applies to publicly accessible venues; requires organisations to:

- Conduct terrorism risk assessments. (ATRA- Anti Terrorism Risk Assessment)
- Include specific security incident scenarios in plans.
- Run staff training and regular drills.
- Establish clear communications for emergencies.

Civil Contingencies Act & Emergency Planning

Category 1 responders (e.g., LCG -as an education provider) under the Civil Contingencies Act LCG must continually review and test the BCPs after emergencies, ensuring:

- Activation protocols
- Training and exercises
- Publicly sharing elements of the plan where appropriate.

The Act requires Category 1 responders to maintain plans to ensure that they can continue to exercise their functions in the event of an emergency so far as is reasonably practicable

DEFINITIONS

Disaster Recovery
Involves a set of plans, tools, and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

Critical Activities
Business activities and processes that must be restored in the event of a disruption to ensure the ability to protect the organisation's assets, meet organisational needs, and satisfy regulations as well as contractual requirements, including sub-contractors assigned on behalf of LCG business. Personal data is secured and if any potential breach of security reported as required through Data Protection Submission Form.

RELATED POLICIES/PROCEDURES/LINKS/DOCUMENTS

Health and Safety Policy
Incident Response Policy
Safeguarding and Prevent Policy
Data Protection Submission / Breach Reporting Procedure
Cyber Security Policy and Acceptable Use
Emergency Evacuation Procedures
Martyn’s Law preparedness guidance (where premises/events are in scope)

REFERENCES (EXTERNAL GUIDANCE)

HSE: Health and Safety at Work etc. Act 1974 – https://www.hse.gov.uk/legislation/hswa.htm

Legislation.gov.uk: Management of Health and Safety at Work Regulations 1999 – https://www.legislation.gov.uk/uksi/1999/3242/contents

HSE: RIDDOR – https://www.hse.gov.uk/riddor/

GOV.UK: Civil Contingencies Act guidance – https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61029/Chapter-6-Business-Continuity-Management_amends_04042012.pdf

ICO: Business continuity, disaster recovery and backups – https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/records-management-and-security/business-continuity-disaster-recovery-and-back-ups/

ICO: Data (Use and Access) Act 2025 – https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/

ICO: 72 hours – how to respond to a personal data breach – https://ico.org.uk/for-organisations/advice-for-small-organisations/personal-data-breaches/72-hours-how-to-respond-to-a-personal-data-breach/

GOV.UK/Home Office: Terrorism (Protection of Premises) Act 2025 (Martyn’s Law) – https://www.gov.uk/government/collections/terrorism-protection-of-premises-bill-2024

ProtectUK: Martyn’s Law overview – https://www.protectuk.police.uk/martyns-law/martyns-law-overview-and-what-you-need-know

UK Parliament: Cyber Security and Resilience (Network and Information Systems) Bill – https://bills.parliament.uk/bills/4035