



Business Continuity Policy

Contents

1. Introduction
2. Scope and Invocation
3. Policy statement
4. Implementation Framework

5. Roles and Responsibilities
6. Methodology
7. Strategy & Recovery
8. Communication & Awareness
9. Training, Testing and Maintenance
10. Review Process
11. Audit and Governance
12. Contact details
13. Related Policies
14. Appendix 1 – Business continuity Analysis and Risk Assessment
15. Appendix 2 – Major Incident Procedure
16. Appendix 3 – Cyber Incident Procedure
17. Appendix 4 – Training Equipment Inventory
18. Appendix 5 – Business Continuity and Incident Log

1. INTRODUCTION

The Civil Contingencies Act 2004 requires the Business to ensure that it has prepared so far as is reasonably practicable, to continue to provide critical activities and an emergency response during any emergency or disruptive event.

The Business Continuity Policy shall be implemented in all departments and locations where the Business has an office or employees.

The aim of the policy is to describe how the Business intends to mitigate the effect of any incident that causes a severe disruption to the working environment or training venues.

Assumptions used to support the Businesses planning process include the following elements:

- Emergencies or threatened emergencies can adversely impact the Businesses ability to continue to support critical activities and provide support to the operations of clients, partners and external agencies.
- When a business continuity event is declared, the Businesses will implement a predetermined plan using trained and equipped personnel.
- Staff and freelance employees and resources located outside the area affected by the emergency or threat will be available as necessary to continue critical activities.
- Normally available staff members may be rendered unavailable by a disaster or its aftermath or may be otherwise unable to participate in the recovery.
- Procedures are sufficiently detailed so someone other than the person primarily responsible for the work can follow them.
- A disaster may require service users, clients, partners and local agencies to function with limited automated support and some degradation of service, until full recovery is made.

2. SCOPE AND INVOCATION

2.1 - A1 Education & Training undertakes activities and services that must be performed, or rapidly and efficiently resumed, in an emergency. While the impact of an emergency cannot be predicted, planning for operations under such conditions can mitigate the impact of the emergency on our people, our office locations and our objectives.

To that end, A1 Education & Training is undertaking a continuous programme of work to prepare a Business Continuity Plan (BCP). Business Continuity Planning is a good business practice and forms part of the fundamental objectives of our organisation as part of its corporate governance regime. The changing threat environment and recent emergencies have created awareness of the need for BCP capabilities that enable services to continue their critical activities across a broad spectrum of emergencies.

The Business Continuity Plans aim to:

- Prioritise people's safety
- Maintain essential services
- Protect Buildings their contents
- Maintain effective communication with customers, learners, trainers and employees
- Protect business and learner information
- Maintain the ability to access essential electronic records
- Recover critical IT systems and services within acceptable timescales • Maintain essential financial and administrative functions

2.2 Key systems:		
System	Primary purpose	Continuity importance
Microsoft Outlook	Email and calendars	Critical
Microsoft Teams	Online meetings and online training	Critical
SharePoint	Business and training document storage	Critical
Xero	Accounting and financial management	Important
Website	Customer information and course bookings	Important
Internet connectivity	Access to cloud systems and communications	Critical
Scanning facilities	Transfer of registers/examination records to SharePoint	Important

2.3 Information and records

Most business records are electronic.

Physical records are limited principally to:

- Course registers.
- Examination papers.
-

These records are subsequently scanned and uploaded to SharePoint.

This reduces the organisation's dependence on physical storage but creates a significant dependency on SharePoint availability and appropriate backup/recovery arrangements.

2.4 Training equipment

Certain courses require specialist training equipment, particularly first aid training.

Trainers retain their own training equipment rather than the organisation maintaining a single central equipment store.

This provides some resilience against loss of the head office but creates a dependency on individual trainers maintaining, transporting and replacing their equipment appropriately.

3. POLICY STATEMENT

Each department will develop, implement and maintain Business Continuity Plans to ensure that the following are achieved:

Development of procedures and information maintained in readiness for use in an incident to enable the Business to continue to deliver its critical activities at an acceptable pre-defined level. A critical activity is defined as the actions needed to deliver key products and services to meet the most important and time sensitive objectives

Departments will prioritise and group their critical activities against the following criteria;

Priority 1 - Disruption to these activities might have an impact on our ability to deliver an emergency response on behalf the Business may result in serious damage to human welfare.

Priority 2 - Disruption to these activities might have an impact resulting in impact or breakdown of local community services, damage to the environment, loss of income to the Business or loss of reputation.

Priority 3 - Activities that do not fall into either of the first two categories

A1 Education & Training will review its business continuity plan(s) at least annually or at more regular intervals dependent on the level of risk or if there has been significant change in the infrastructure of a service. Testing must take place either annually or biennially depending on the type of plan. The Directors are, overall, responsible for ensuring that the management of business continuity is incorporated in the Businesses processes and structure. Senior Leadership Team are responsible for ensuring that all services comply with this policy.

4. IMPLEMENTATION FRAMEWORK

The delivery of business continuity management will be based on a principle of central support for a local delivery. Each service will have a nominated business continuity coordinator. They will identify those within their services who will undertake a business impact analysis and prepare the service recovery plan.

5. ROLES AND RESPONSIBILITIES

Directors and Senior Leadership will:

- Act to ensure/monitor the overall strategic direction of Business Continuity Management across all operations
- Ensure that the Business Continuity Management Policy and development plan is enforced and resourced appropriately for the benefit of all parts of the organisation
- In the event of a serious or widespread disruption to the activities of the Business, it may be necessary for the Health & Safety and Safeguarding Manager to take charge.
- Undertake leadership of the Business Continuity assessments and plans under the direction of the Director for Quality, Curriculum and Compliance.
- Act as a point of tactical leadership in support of activities
- Either make decisions regarding assessments and recommendations provided or refer upwards for a decision

- Support services in exercising Business Continuity Plans at both corporate and business levels
- Manage, monitor and report on the progress of the Business Continuity Management Strategy and Delivery Plan as required
- In collaboration with other category 1 responders as defined by the Civil Contingencies Act, make arrangements to promote Business Continuity awareness, advice and assistance to delivery partners
- Ensure that where appropriate, sections of Business Continuity Plans are published and accessible to the public
- Make arrangements to support departments in undertaking risk and business impact analysis

Directors and Senior Leadership are responsible for undertaking or delegating:

- Business impact analysis for their area of responsibility
- Preparing a Service Recovery Plan for their area
- Ensuring that arrangements are made to test, maintain and review service recovery plans that are their responsibility
- Allocate business continuity objectives to managers in the service
- Nominate one manager/staff member who will have specific responsibility for business continuity in their department
- Allocate sufficient resources to the nominated BCM coordinators for development, training, rehearsals and maintenance of business continuity plans.
- Ensure that departmental business continuity risk assessments and arrangements are regularly reviewed
- Report on service continuity performance as required

BCM Coordinators:

Each department is responsible for producing its own business continuity plans at a service delivery and service recovery level. The coordinator will therefore:

- Manage and co-ordinate the business continuity activities of the department in compliance with the corporate business continuity policy.
- Ensure that written business continuity recovery plans are produced and kept current
- Ensure that the completed plans are periodically tested
- To convene any subgroups and support teams that will be required to develop and deliver the objectives and priorities

6. METHODOLOGY

Risks will be assessed using a 5 × 5 scoring system.

6.1 Likelihood:

Score	Description
1	Rare – highly unlikely to occur
2	Unlikely – could occur but not expected regularly

3	Possible – could occur from time to time
4	Likely – expected to occur periodically
5	Almost certain – expected to occur frequently

6.2 Impact

Score	Description
1	Insignificant – minimal operational impact
2	Minor – short disruption with limited consequences
3	Moderate – significant disruption requiring management action
4	Major – serious disruption affecting customers/business
5	Severe – prolonged or potentially critical business impact

6.3 Risk rating

Risk score = Likelihood × Impact

Score	Rating	Required response
1–4	Low	Manage through normal controls
5–9	Moderate	Management attention and appropriate controls
10–16	High	Additional controls/action required
17–25	Critical	Immediate management attention and continuity planning

7. STRATEGY AND RECOVERY

The BCP is applicable to all the business's services, departments, partners, contractors and personnel. The BCP can be activated during duty and non-duty hours, both with and without warning. The BCP covers all locations, systems and buildings operated or maintained by the Business. The BCP supports the performance of critical activities from alternate locations (due to the primary location becoming unusable, for long or short periods of time) and provides for continuity of management and decision-making, in the event that senior management or delivery personnel are unavailable.

The BCP will be distributed to senior managers within the Business. Appropriate training will be provided to personnel with identified responsibilities.

8. COMMUNICATION & AWARENESS

The Business Continuity Management Policy and other supporting information is placed in appropriate places within our premises and is actively promoted by management teams to both new starters as part of the induction process and existing staff.

Promoting business continuity awareness throughout the organisation will primarily be achieved through workshops and regular updates via email.

9. TRAINING, TESTING AND MAINTENANCE

Training: It will be obligatory for employees to take part in regular training and exercising as required. Organising such training or test is the responsibility of Directors or their delegated representative. The training will take place at a time when its effect on our customers or clients is minimal.

Rehearsals: To make the plans effective, regular testing is required. The results of the tests will be reported to the Senior Leadership team. In case of unsatisfactory results, the reasons are determined and alterations may be made to the relevant part of the Business Continuity Plan.

Maintenance: To keep the plans up-to-date and current, alterations may be necessary when procedural changes to service operations occur or when new threats arise; therefore, the maintenance of the plans is an on-going process.

10. REVIEW PROCESS

The key Business Continuity Risk Assessments and Plans will be completed as soon as possible and reviewed annually to ensure that information on service functions, contacts and telephone information are kept up to date. In addition, a programme of testing and exercising will be developed.

Any lessons learned from training, exercising or indeed invocation will be incorporated into the rolling annual review process.

A debrief is a review that is carried out following an incident when all persons involved can be present.

The debrief will ideally be arranged as soon as possible by the Incident Lead to get an accurate and reliable account of what happened and to allow for important lessons to be identified.

1. The person co-ordinating the incident needs to attend as well as key members of the incident team.
2. Appoint a facilitator, ideally someone who was not closely involved in the incident who can ask questions from an independent and non-biased perspective. The facilitator should be briefed to allow them to delve in more depth into key positives and criticisms.

3. Go through the incident response step by step. Revisit the emergency plan and identify any deviation from plan. What changed and why?

4. Ask for specific feedback on a series of headings based on the key issues/areas for example:

- Procedures
- Communication
- Liaison
- Finance
- Public Relations
- Health and Safety
- Resources

The key questions to address are:

- What went well?
- What didn't go so well?
- What would we do if we were in the situation again?

5. Use the Example Agenda for an Incident Debrief as a guide

6. Complete a report to document recommendations and opportunities for improvement and any lessons identified. It is important that the Directors or Chair of Governors takes ownership of the report to ensure that any actions are taken forward.

11.AUDIT AND GOVERNANCE

BCM arrangements form part of the Businesses overall internal control environment, which are subject to annual review as part of the organisation's Self-Assessment.

12. CONTACT DETAILS

Name: Emma Merrick

Job Title: Director

Tel: 07834 731914

Email Address: Emma.merrick@a1-training.co.uk

Name: Rebecca Lander

Job Title: Director and Quality Lead

Tel: 07518 906136

Email Address: becca.lander@a1-training.co.uk

13. RELATED POLICIES

- Confidentiality
- Data Protection and GDPR (including security of assessment papers)
- Health and Safety
- Lone working
- Safeguarding



Business Continuity Analysis and Risk Assessment

CONTENTS

1. Critical business activities

2. Initial recovery priorities
3. Business continuity risk register
4. Principal business continuity risks
5. Proposed recovery objectives
6. Immediate control improvement programme
7. Business continuity structure
8. Supporting documents

1. Critical business activities

Priority	Business activity	Impact if unavailable
1	Training delivery	Loss of revenue, customer dissatisfaction, contractual impact and potential reputational damage
2	Trainer availability and allocation	Inability to deliver scheduled training

3	Customer communication	Customers may not receive changes, cancellations or important information
4	Course scheduling/booking	Courses may be missed, incorrectly scheduled or unable to proceed
5	Access to training materials	Training quality and delivery may be affected
6	Access to learner/course records	Compliance, certification and customer requirements may be affected
7	Online training	Virtual courses cannot be delivered
8	Financial administration	Invoices, payments and financial management may be disrupted
9	Website/course booking	New bookings and customer enquiries may be affected
10	Management/incident coordination	Organisation may struggle to coordinate an effective response

2. Initial Recovery Priorities

The following recovery priorities are agreed.

Priority 1 – Immediate

- Protection of people and safety.
- Establishment of incident management.
- Contact with affected trainers/customers.
- Restoration of essential communications.
- Identification of scheduled training affected by the incident.

Priority 2 – Within 24 hours

- Access to essential training information.
- Trainer allocation and scheduling.
- Customer communication.
- Alternative arrangements for affected courses.
- Online training capability where appropriate.

Priority 3 – Within 48–72 hours

- Restoration of routine administration.
- Financial administration.

- Website/booking functionality.
- Recovery of non-critical information and processes.

Priority 4 – Longer-term

- Restoration of normal office arrangements.
- Replacement of damaged/lost equipment.
- Completion of outstanding administration.
- Post-incident review.

3. Business Continuity Risk Register

ID	Risk	Likelihood	Impact	Initial Rating	Key existing controls
BC-01	Loss of head office	2	3	Moderate	Staff can work remotely; training generally delivered at customer venues
BC-02	Loss of Microsoft 365 access	3	5	High	Cloud-based systems; staff use Microsoft 365. Backups made by IT
BC-03	Cyberattack/account compromise	3	5	High	IT support, cyber incident procedure
BC-04	Loss of SharePoint access	2	5	High	Electronic document storage, Backups made by IT
BC-05	Loss of Teams	3	4	High	Face-to-face delivery available, phone calls and Teams on work phones
BC-06	Loss of Outlook/email	3	5	High	Microsoft 365, Use of personal emails and phones if required in an emergency
BC-07	Loss of internet connectivity	3	4	High	Staff can work from different locations; Staff can use work phones for internet access
BC-08	Loss of Xero	2	3	Moderate	Cloud accounting system, weekly backups made by Directors

ID	Risk	Likelihood	Impact	Initial Rating	Key existing controls
----	------	------------	--------	----------------	-----------------------

BC-09	Loss of key trainer	3	4	High	Trainers plus freelancers
BC-10	Widespread trainer absence	3	5	High	Freelance trainer network
BC-11	Freelance trainer unavailability	3	4	High	Employee trainers available
BC-12	Customer venue unavailable	4	4	High	Training delivered at customer alternative premises – customers responsibility
BC-13	Severe weather / transport disruption	3	4	High	Online delivery available for some courses
BC-14	Loss of training equipment	3	4	High	Trainers generally hold own equipment, Equipment inventory in place for all A1 Education and Training equipment, equipment can be shared as required
BC-15	Training materials unavailable	2	4	Moderate	SharePoint storage, access via backups or through awarding organisations websites
BC-16	Physical course records lost before scanning	2	3	Moderate	Records subsequently scanned within 24 hours. Any losses will require trainer to obtain the necessary information again
BC-17	Website unavailable	2	3	Moderate	Direct customer communication available
BC-18	Loss of course booking capability	2	4	Moderate	Manual communication possible
BC-19	Loss of IT support resource	3	4	High	Internal colleague provides IT support
BC-20	Major supplier failure	2	4	Moderate	Alternative suppliers are available
BC-21	Major national incident	2	5	High	Remote/online delivery capability
BC-22	Loss/corruption of business data	2	5	High	SharePoint/cloud storage

BC-23	Loss of financial administration	2	3	Moderate	Xero, weekly backups made by Directors
BC-24	Loss of communications with customers	3	5	High	Outlook/Teams, Emergency contact list maintained by Senior Leadership team
ID	Risk	Likelihood	Impact	Initial Rating	Key existing controls
BC-25	Failure to coordinate an incident	3	5	High	Informal management arrangements in place (Major incident protocol)

4. Principal Business Continuity Risks

The assessment indicates that the organisation's most significant continuity exposures are not primarily associated with the physical head office.

The principal exposures are:

4.1 People

The organisation is heavily dependent upon its employee trainers and its freelance trainer network.

Although there is no single individual whose absence would cause a major business failure, widespread absence could substantially reduce the organisation's ability to fulfil scheduled training.

Required controls:

- Maintain a current trainer skills matrix.
- Identify courses each trainer is qualified/competent to deliver.
- Maintain an approved freelance trainer list.
- Identify backup trainers for critical courses.
- Establish a process for prioritising customer bookings during staff shortages.

4.2 Microsoft 365

Outlook, Teams and SharePoint are critical to daily operations.

A loss of access could affect:

- Customer communications.
- Training schedules.
- Online training.
- Internal communications.
- Training materials.

- Learner records.
- Management information.

4.3 Customer venues

Because much of the organisation's face-to-face training takes place at customer premises, the organisation does not have to maintain large alternative training facilities.

However, venue disruption could occur at short notice.

The BCP should provide three primary options:

1. Alternative customer venue.
2. Remote/online delivery where the course permits.
3. Rescheduling.

4.4 Training equipment

The decentralised ownership of training equipment provides some resilience because equipment is not all held at the head office.

However, equipment availability should be incorporated into course planning.

A basic equipment inventory and replacement/contingency process is in place, particularly for first aid courses.

4.5 Records and information

The organisation is predominantly electronic, which is beneficial for continuity but creates a high dependency on access to SharePoint.

Data is backed up by IT support on a regular basis, and this allows for the recovery of data in cases of accidental deletion and recovery from malicious deletion/ransomware.

5. Proposed Recovery Objectives

The following are agreed Maximum Tolerable Periods of Disruption (MTPD) and Recovery Time Objectives (RTO)		
Service/activity	MTPD	RTO
Incident management	1 hour	1 hour
Customer communication	4 hours	2 hours
Trainer scheduling	8 hours	4 hours
Scheduled critical training	24 hours	24 hours

Online training capability	24 hours	24 hours
Access to critical training documents	24 hours	12 hours
Learner/course records	48 hours	24 hours
Financial administration	5 working days	3 working days
Website/online booking	5 working days	3 working days
Service/activity	MTPD	RTO
Routine administration	5 working days	3 working days

6. Immediate Control Improvement Programme

The following actions are to always be in place:

Priority	Action	Target
1	Approval Business Continuity Policy	Senior Management High
2	Appointed Business Continuity Lead	Senior Management High
3	Access to a Management/Admin emergency contact list	High
4	Maintain up to date Training Management availability matrix	High
5	Maintain approved Training Management contingency list	High
6	Maintain details of employee and freelance contact details outside of Microsoft 365	High

7. Business Continuity Structure

Business Continuity Lead – Emma Merrick Tel: 07834 731914 Email
Address: Emma.merrick@a1-training.co.uk

Responsible for:

- Activating the BCP.
- Assessing the incident.
- Coordinating the response.
- Making or escalating key decisions.
- Maintaining the incident log.
- Coordinating recovery.

Operations/Training Lead – Becca Lander Tel: 07518 906136 Email
Address: becca.lander@a1-training.co.uk

Responsible for:

- Identifying affected courses.
- Assessing trainer availability.
- Finding alternative trainers.
- Identifying alternative delivery arrangements.
- Coordinating customer requirements.
- Customer communications.
- Learner communications.
- Course records.
- Booking changes.
- Maintaining relevant administrative information.

IT Lead/Support – Joe Foden – fodo1999@gmail.com

Responsible for:

- Assessing IT incidents.
- Microsoft 365 access.
- Cyber incidents.
- Data recovery.
- Escalating to external IT support where required.

8. Supporting Documents

This risk assessment is a part of the foundation for the wider Business Continuity Management System consisting of:

1. **Business Continuity Policy**
2. **Major Incident Procedure**
3. **Cyber Incident Procedure**
4. **Training Equipment Inventory**
5. **Business Continuity and Incident inventory**

APPENDIX 2



Major Incident procedure

CONTENTS

1. Purpose
2. Scope
3. Definition of a Major Incident
4. Incident Management Principles
5. Incident Management Structure
6. Emergency Procedures
7. Incident Levels
8. Initial Response – First 15 Minutes
9. Initial Incident Assessment
10. Activation of the Business Continuity Plan
11. Establish the Incident Team
12. Incident Log
13. Communication During a Major Incident
14. Communication Priority
15. Loss of Head Office
16. IT or Cyber Incident
17. Loss of Trainers or Widespread Staff Absence
18. Customer Venue Incident
19. Training Equipment Incident
20. Severe Weather or Transport Disruption
21. Maintaining Critical Training
22. Customer Communication
23. Staff Welfare
24. Decision Making
25. External Support

- 26. Recovery
- 27. Stand Down Criteria
- 28. Post Incident Review
- 29. Major Incident Checklist
- 30. Testing and Exercising
- 31. Supporting Documents

1. Purpose

This procedure sets out how the organisation will respond to a major incident that could significantly affect its people, customers, training delivery, premises, systems, information or reputation.

The organisation operates nationally and delivers health and social care, residential childcare and health and safety training through a combination of face-to-face and online delivery.

Because the organisation has 15 employees, all of whom have training responsibilities, the procedure uses a **simple, flexible incident management structure** rather than a large emergency management hierarchy.

The objectives are to:

- Protect people from harm.
 - Establish effective control of the incident.
 - Maintain essential business operations.
 - Minimise disruption to customers and learners.
 - Protect business and personal information.
 - Maintain effective communications.
 - Activate business continuity arrangements where necessary. • Recover critical services as quickly as reasonably practicable.
 - Ensure appropriate regulatory, contractual and insurance requirements are considered.
 - Learn from incidents and improve organisational resilience.
-

2. Scope

This procedure applies to all employees and should also be communicated to freelance/associate trainers where relevant.

It applies to major incidents including, but not limited to:

- Serious injury, illness or death affecting staff or learners.
- Fire or significant damage to premises.
- Loss of the head office.
- Major IT or Microsoft 365 outage.
- Cyber-attack or ransomware.
- Significant data breach.
- Widespread loss of trainers/staff.
- Severe weather.
- Major transport disruption.
- Customer venue disruption affecting multiple courses.
- Loss of critical training equipment.
- Major supplier failure.
- Loss of critical business information.
- Major financial incident.
- Significant reputational incident.

- National or regional emergency affecting training delivery.
 - Any other event that management considers capable of causing significant disruption.
-

3. Definition of a Major Incident

A major incident is an event that has, or is likely to have, a significant impact on the organisation's ability to operate normally and requires coordinated management action.

An incident should be treated as potentially major where it:

- Threatens life or safety.
- Affects multiple employees or customers.
- Prevents delivery of a significant number of courses.
- Affects a critical business system.
- Involves significant or potentially significant loss of personal/business information.
- Causes prolonged loss of premises.
- Creates significant financial or contractual exposure.
- Is likely to cause significant reputational damage.
- Requires external emergency services or specialist assistance.
- Cannot be managed effectively through normal business arrangements.

When in doubt, escalate.

4. Incident Management Principles

The organisation will follow these principles:

6. **People first.**
 7. **Assess before acting.**
 8. **Establish clear leadership.**
 9. **Communicate accurate information.**
 10. **Maintain essential services where possible.**
 11. **Protect information and evidence.**
 12. **Do not speculate.**
 13. **Document significant decisions.**
 14. **Use alternative arrangements where normal processes are unavailable.**
 15. **Return to normal operations in a controlled manner.**
-

5. Incident Management Structure

The organisation should nominate people to the following roles and maintain named deputies.

5.1 Incident Lead

The Incident Lead has overall responsibility for coordinating the organisational response.

Responsibilities include:

- Assessing the incident.
- Activating this procedure.
- Deciding whether the Business Continuity Plan should be activated.
- Establishing priorities.
- Coordinating staff.
- Coordinating external support.
- Approving significant communications.
- Maintaining oversight of customer impact.
- Recording key decisions.
- Authorising stand-down.
- Maintaining customer and learner information.
- Supporting communications.
- Maintaining records.
- Recording course changes.
- Maintaining the incident log.

5.2 Deputy Incident Lead

The Deputy assumes the Incident Lead role when the Incident Lead is unavailable.

5.3 Training/Operations Lead

Responsible for:

- Identifying affected courses.
- Identifying affected trainers.
- Reallocating trainers.
- Identifying alternative delivery arrangements.
- Contacting affected customers where delegated.
- Assessing equipment and venue requirements.

5.4 IT Support Lead

Responsible for:

- Assessing IT incidents.
 - Managing technical recovery.
 - Coordinating cyber response.
 - Assessing Microsoft 365, SharePoint, Teams and other system availability.
 - Escalating to external IT/cyber specialists where necessary.
-

6. Emergency Services

Where there is an immediate threat to life, serious injury, fire, crime or another emergency requiring urgent assistance, the appropriate emergency service should be contacted immediately.

The organisation's internal procedures must not delay emergency assistance.

Once immediate safety has been addressed, the Incident Lead should be notified.

7. Incident Levels

Level	Description	Response
Level 1 – Routine	Can be managed through normal procedures	Local response
Level 2 – Significant	Requires management coordination	Incident Lead informed
Level 3 – Major	Significant operational/customer impact	Major Incident Procedure activated
Level 4 – Critical	Severe or widespread impact	Major Incident Procedure + BCP fully activated
The level may be changed as information develops.		

8. Initial Response – First 15 Minutes

The person discovering the incident should:

16. Protect themselves and others from immediate danger.
17. Contact emergency services where necessary.
18. Notify the Incident Lead or deputy.
19. Provide factual information.
20. Do not speculate about causes or consequences.
21. Follow immediate instructions.
22. Preserve relevant information/evidence where safe to do so.

The Incident Lead should establish:

- What happened
- When did it happen
- Where did it happen
- Who is affected
- Is anyone in immediate danger
- What services are affected
- What training is affected

- What information/systems are affected
 - Is the incident continuing
 - What immediate action is required
-

9. Initial Incident Assessment

The Incident Lead should assess the incident against:

People

- Are staff safe?
- Are learners/customers safe?
- Is anyone injured or missing?
- Is there a welfare concern?

Operations

- Which courses are affected?
- Which trainers are affected?
- Which customer venues are affected?
- Can training continue?

Technology

- Are Microsoft 365 systems available?
- Is Outlook available?
- Is Teams available?
- Is SharePoint available?
- Is Xero available?
- Is the website available?

Information

- Has business or personal information been lost?
- Has information potentially been accessed by an unauthorised person?

Premises/equipment

- Is the head office available?
- Is essential training equipment available?

Customers

- Which customers need immediate contact?
 - Are contractual commitments affected?
-

10. Activation of the Business Continuity Plan

The Incident Lead should activate the Business Continuity Plan where the incident is likely to:

- Prevent normal delivery of critical training.
- Affect multiple courses.

- Affect critical IT systems.
- Prevent access to critical records.
- Prevent normal communication.
- Cause prolonged loss of premises.
- Cause significant staff/trainer absence.
- Create significant customer or contractual impact.
- Require alternative working arrangements.

The decision and time of activation should be recorded.

11. Establish the Incident Team

Once activated, the Incident Lead should identify the people required to manage the incident.

The team should be kept as small as practicable.

The Incident Lead should assign:

- Incident management.
- Training/operations.
- IT.
- Customer communications.
- Administration/records.

Additional people should be involved only where required.

12. Incident Log

The A1 Education and Training's Business Continuity and Incident Log is to be fully completed as soon as is possible.

The log should record significant:

- Decisions.
- Actions.
- Communications.
- System changes.
- Customer impacts.
- Recovery actions.
- External contacts.

The log should be stored securely and, where the incident involves IT systems, separately from the affected systems where practicable.

13. Communication During a Major Incident

Communication should be:

- Prompt.
- Factual.
- Clear.
- Consistent.
- Appropriate to the audience.

Potential audiences include:

- Employees.
- Freelance trainers.
- Customers.
- Learners.
- Suppliers.
- Professional/accreditation bodies.
- Insurers.
- Regulators.
- Relevant authorities.

Only authorised personnel should issue external statements about significant incidents.

Employees and trainers should not make public statements or post incident information on social media without authorisation.

14. Communication Priority

Priority 1

People directly affected or at immediate risk.

Priority 2

Employees and trainers required to respond.

Priority 3

Customers and learners affected by training disruption.

Priority 4

Suppliers and other relevant stakeholders.

Priority 5

Wider communications, where necessary.

15. Loss of Head Office

If the head office is unavailable:

- Confirm whether anyone is at risk.
- Do not enter an unsafe building.
- Establish alternative working arrangements.
- Direct staff to work from home where appropriate.
- Move essential administrative activity to remote working.
- Identify any physical records or equipment that may be affected.
- Contact insurers/property providers where appropriate.
- Assess whether the office can be safely reoccupied.
- Identify temporary premises if required.

Because the organisation already operates through home-based staff and customer venues, **remote working should be the initial continuity arrangement wherever practical.**

16. IT or Cyber Incident

If the major incident involves IT or cyber security:

The **Cyber Incident Procedure** must be activated.

This should:

- Protect affected systems.
- Contact IT support.
- Preserve evidence.
- Secure compromised accounts.
- Assess customer/training impact.
- Assess potential data protection implications.
- Establish alternative communication arrangements.
- Activate business continuity arrangements if critical systems are unavailable.

Staff should not attempt unauthorised technical recovery.

17. Loss of Trainers or Widespread Staff Absence

If staff/trainer availability is significantly reduced:

The Training/Operations Lead should:

23. Identify all affected courses.
24. Identify essential/priority courses.
25. Identify available employee trainers.
26. Contact approved freelance/associate trainers.

27. Reallocate trainers where appropriate.
28. Determine which courses can be delivered online.
29. Contact customers where arrangements cannot be maintained.
30. Reschedule lower-priority courses where necessary.

Training should be prioritised based on:

- Customer urgency.
 - Contractual commitments.
 - Regulatory requirements.
 - Learner impact.
 - Availability of suitably competent trainers.
 - Availability of equipment.
-

18. Customer Venue Incident

If a customer venue becomes unavailable:

Consider, in order:

31. Alternative room/venue at the customer premises.
32. Alternative venue.
33. Online delivery, where suitable.
34. Alternative trainer if the original trainer is affected.
35. Rescheduling.

The customer should be contacted as soon as practicable.

No alternative delivery arrangement should compromise learner safety, training quality or applicable course requirements.

19. Training Equipment Incident

If essential equipment is unavailable:

- Identify the affected course.
- Determine whether the equipment is essential.
- Check availability of alternative equipment.
- Check whether another trainer has suitable equipment.
- Consider hiring/purchasing replacement equipment.
- Consider alternative delivery.
- Reschedule if necessary.

The Training Equipment Inventory and Continuity Register should be used.

20. Severe Weather or Transport Disruption

The Incident Lead/Training Lead should assess:

- Staff safety.
- Trainer ability to travel.
- Customer venue availability.
- Learner ability to attend.
- Road/rail disruption.
- Whether online delivery is possible.

Safety takes priority over maintaining the original delivery arrangement.

Training should be postponed where travel would create an unacceptable risk.

21. Maintaining Critical Training

During a major incident, the A1 Education & Training will establish a list of affected courses.

Course	Customer	Date/time	Trainer	Delivery method	Equipment	Status	Action

Each affected course should be classified:

Green: Continue as planned.

Amber: Continue with changes.

Red: Unable to continue; alternative arrangement required.

22. Customer Communication

Where training is affected, the Quality Lead will provide:

- Confirmation that an operational issue has occurred.
- The course/date affected.
- The impact on the customer.
- The proposed alternative.
- Any action required from the customer.
- Contact details for further information.
- Expected time for the next update.

Staff should not provide unverified explanations of the cause.

23. Staff Welfare

During a major incident, management should consider:

- Physical safety.
- Workload.
- Stress and fatigue.
- Travel safety.
- Additional responsibilities placed on staff.
- Need for time away from work.
- Support required following a distressing incident.

No employee should be expected to undertake work that places them at unreasonable risk.

24. Decision Making

When information is incomplete, decisions will be based on:

1. Safety.
2. Legal/regulatory requirements.
3. Protection of personal/business information.
4. Continuity of critical training.
5. Customer impact.
6. Financial impact.
7. Reputational impact.
8. Practicality and available resources.

Important decisions should be recorded in the incident log.

25. External Support

Depending on the incident, management may need to contact:

- IT/cyber support.
- Insurance provider.
- Legal advisers.
- Relevant authorities.
- Data protection advisers.
- Awarding/accreditation bodies.
- Key suppliers.
- Property/landlord contacts.
- Customers.

26. Recovery

The Incident Lead will coordinate recovery in stages.

Stage 1 – Stabilise

- Protect people.
- Contain the incident.
- Prevent further damage.

Stage 2 – Maintain

- Maintain critical training.
- Establish alternative working arrangements.
- Communicate with affected customers.

Stage 3 – Recover

- Restore systems.
- Replace equipment.
- Restore normal premises arrangements.
- Recover outstanding administration.

Stage 4 – Return to normal

- Confirm normal services.
 - Close temporary arrangements.
 - Complete outstanding records.
 - Stand down the incident team.
-

27. Stand-Down Criteria

The Incident Lead may stand down the Major Incident Procedure when:

- Immediate risks have been controlled.
- People are safe.
- Critical training delivery has resumed, or acceptable arrangements are in place.
- Essential systems have been restored or suitable alternatives established.
- Customers have been appropriately informed.
- Outstanding regulatory or data protection actions have been transferred to normal management processes.
- Recovery actions have been assigned.

The stand-down decision should be recorded.

28. Post-Incident Review

A formal review should take place following every Level 3 or Level 4 incident.

The review should consider:

What happened?

- What was the incident?
- When was it identified?
- How long did it last?

What was the impact?

- People.
- Customers.
- Learners.
- Training.
- IT.
- Information.
- Finances.
- Reputation.

How effective was the response?

- Was the incident identified quickly?
- Was the correct person contacted?
- Was the BCP activated appropriately?
- Were communications effective?
- Were customers supported?
- Were recovery objectives achieved?

What needs to improve?

- Procedures.
- Training.
- IT controls.
- Equipment.
- Staffing.
- Communications.
- Supplier arrangements.

Actions should be recorded with an owner and target completion date.

29. Major Incident Checklist

Immediate response

- ☐ Protect people and ensure immediate safety.
- ☐ Contact emergency services if required.
- ☐ Notify Incident Lead.

- ☐ Establish what has happened.
- ☐ Identify people affected.
- ☐ Identify immediate business impact.
- ☐ Establish whether the incident is continuing.
- ☐ Assign incident responsibilities.
- ☐ Start incident log.

Business continuity

- ☐ Decide whether to activate the BCP.
- ☐ Identify affected training. ☐
- Identify affected trainers.
- ☐ Identify affected customers.
- ☐ Assess IT/system availability.
- ☐ Establish alternative working arrangements.
- ☐ Establish alternative training arrangements.
- ☐ Contact affected customers.
- ☐ Prioritise critical services.

Recovery

- ☐ Confirm immediate threat has been controlled.
 - ☐ Restore critical systems/services.
 - ☐ Replace essential equipment.
 - ☐ Confirm training delivery has resumed.
 - ☐ Complete required communications.
 - ☐ Transfer outstanding actions to responsible owners.
 - ☐ Stand down incident response.
 - ☐ Complete post-incident review.
 - ☐ Update risk assessment/BCP where required.
-

30. Testing and Exercising

This procedure will be tested at least annually.

Suggested exercises include:

Exercise 1 – Loss of premises

The Shrewsbury head office becomes unavailable for five working days.

Exercise 2 – Cyber incident

A trainer's Microsoft 365 account is compromised, and suspicious emails are sent to customers.

Exercise 3 – Widespread trainer absence

Approximately 40% of trainers become unavailable during a period of high customer demand.

Exercise 4 – Customer venue failure

Multiple customer venues become unavailable on the same day.

Exercise 5 – Major IT outage

Microsoft 365 becomes unavailable for 24 hours while online training is scheduled.

Following each exercise:

- Record what happened.
 - Identify weaknesses.
 - Assign corrective actions.
 - Update procedures.
 - Report findings to management.
-

31. Supporting Documents

This risk assessment is a part of the foundation for the wider Business Continuity Management System consisting of:

1. **Business Continuity Policy**
2. **Business Continuity Analysis and Risk Assessment**
3. **Cyber Incident Response Procedure**
4. **Training Equipment Inventory**
5. **Business Continuity and Incident Log**

APPENDIX 3



Cyber Incident Procedure

CONTENTS

1. Purpose
2. Scope
3. What is a Cyber Incident
4. Core Principles

5. Roles and Responsibilities
6. Incident Severity
7. Immediate Response – First 15 Minutes
8. If a Device is Lost or Stolen
9. Compromised Microsoft 365 Account
10. Ransomware or Malware
11. Suspected Data Breach
12. Loss of Microsoft 365
13. SharePoint Incident
14. Xero Incident
15. Website or Online Booking Incident
16. Customer and Learner Communications
17. Business Continuity Activation
18. Maintaining Training Delivery
19. Evidence and Incident Records
20. Recovery
21. Return to Business as Usual
22. Post-Incident Review
23. Cyber Incident Contact List
24. Preventative Controls
25. Testing
26. Employee Quick Reference
27. Supporting documents

1. Purpose

This procedure establishes the actions to be taken if A1 Education & Training experiences, or suspects that it has experienced, a cyber security incident.

The purpose is to:

- Protect employees, customers, learners and business information.
- Contain and minimise the impact of a cyber incident.
- Protect Microsoft 365, SharePoint, Outlook and Teams.
- Protect Xero, the website and other business systems.
- Maintain essential business operations.
- Preserve evidence where appropriate.
- Ensure incidents are escalated and reported appropriately.
- Restore affected services safely.
- Support compliance with data protection and contractual requirements.
- Provide a consistent response rather than relying on individual judgement.

This procedure forms part of the organisation's Business Continuity Plan.

2. Scope

This procedure applies to all employees, freelance trainers and other individuals who have access to the organisation's systems or information.

It applies to incidents involving:

- Microsoft 365.
- Outlook/email.
- Teams.
- SharePoint.
- Xero.
- Website and online booking systems.
- Computers, laptops, tablets and mobile devices.
- Business and learner data.
- Passwords and user accounts.
- Cloud services.
- Removable media.
- Phishing and social engineering.
- Malware or ransomware.
- Unauthorised access.
- Lost or stolen devices.
- Accidental disclosure of information.
- Suspected data breaches.
-

3. What is a Cyber Incident?

A cyber incident is any event that could compromise the confidentiality, integrity or availability of the organisation's systems or information.

Examples include:

- A suspicious email or phishing message.
- A compromised Microsoft 365 account.
- A password being disclosed.
- Unauthorised access to SharePoint.
- Malware or ransomware.
- A suspicious login.
- Loss or theft of a company device containing business information.
- Accidental emailing of personal or confidential information to the wrong recipient.
- Unauthorised deletion or alteration of files.
- Unexplained changes to documents.
- Loss of access to business systems.
- A cyber-attack against the website.
- A suspected data breach.

If in doubt, report it. Employees and trainers should not attempt to decide whether an event is “serious enough” to report.

4. Core Principles

During a cyber incident, staff should:

9. **Stop and report.**
10. **Do not investigate beyond what is necessary to protect the organisation.**
11. **Do not delete evidence.**
12. **Do not communicate details of the incident externally unless authorised.**
13. **Do not attempt to negotiate with attackers.**
14. **Do not make assumptions about whether information has been accessed.**
15. **Follow instructions from the Incident Lead and IT support.**
16. **Record important actions and decisions.**

5. Roles and Responsibilities

5.1 Incident Lead

The Incident Lead is responsible for:

- Determining whether the Cyber Incident Procedure should be activated.
- Coordinating the organisational response.
- Ensuring appropriate people are informed.
- Maintaining an incident log.
- Coordinating business continuity arrangements.
- Escalating serious incidents to senior management.
- Approving external communications.

5.2 IT Support Lead

The IT Support Lead is responsible for:

- Assessing the technical incident.
- Securing affected accounts and devices.
- Working with Microsoft/appropriate service providers where required.
- Preserving technical evidence.
- Restoring systems safely.
- Advising the Incident Lead about technical risks.
- Escalating to external cyber/IT specialists where necessary.

5.3 Management

Management is responsible for:

- Making strategic decisions.
- Authorising significant expenditure.
- Determining whether business continuity arrangements need to be activated.
- Considering regulatory, contractual, insurance and reputational implications.
- Approving significant external communications. [5.4 All Employees and](#)

Trainers All personnel must:

- Report suspected incidents immediately.
- Follow IT and management instructions.
- Protect passwords and authentication information.
- Avoid spreading information about the incident.
- Preserve relevant evidence.

Cooperate with investigation and recovery.

6. Incident Severity

The Incident Lead should initially classify incidents as follows.

Level	Description	Example
-------	-------------	---------

•

Level 1 – Minor	Limited incident with minimal business impact	Single phishing email reported before interaction
Level 2 – Significant	Actual or suspected compromise requiring management/IT action	Compromised user account
Level 3 – Major	Significant business disruption or potential data breach	Ransomware, widespread account compromise or major data exposure
Level 4 – Critical	Serious/prolonged disruption affecting core operations or involving significant personal data/security consequences	Major cyber-attack affecting multiple critical systems

7. Immediate Response – First 15 Minutes

Anyone discovering or suspecting a cyber incident should:

If an email appears suspicious

- Do not click further links.
- Do not open additional attachments.
- Do not reply to the sender.
- Report the message using the organisation's approved Microsoft 365 reporting facility, where available.
- Inform IT support if there is any possibility that a link or attachment was opened. **If a link or attachment has already been opened** Immediately:

17. Stop interacting with the message.
18. Disconnect the affected device from the internet if instructed by IT support.
19. Do not delete the email or files.
20. Do not restart or wipe the device unless instructed.
21. Contact IT support.
22. Provide details of what happened and when.

If a password may have been compromised Inform

IT support immediately.

Do not reuse the compromised password.

IT support should assess whether the account needs to be secured, including password reset, session revocation and additional authentication measures.

8. If a Device is Lost or Stolen

The employee/trainer must report the loss immediately.

The following information should be provided:

- Name of person responsible for the device.
- Device type.
- Approximate time and location of loss.
- Whether the device was encrypted, if known.
- Whether the device was logged into Microsoft 365.
- Whether sensitive or personal information may have been accessible.

IT support should consider:

- Blocking access.
- Revoking active sessions.
- Changing credentials where appropriate.
- Remote locking or wiping, if available.
- Assessing potential information exposure.

Where theft is suspected, management should consider whether a police report or insurer notification is appropriate.

9. Compromised Microsoft 365 Account

If an account is suspected of being compromised:

IT Support should:

- Disable or secure the account where appropriate.
 - Reset credentials.
 - Revoke active sessions/tokens where appropriate.
 - Review recent sign-in activity.
 - Review suspicious email activity.
- Check for unauthorised forwarding rules.

•

-
-
-
-

Check mailbox activity.

Check SharePoint/OneDrive activity where relevant.

Review changes to account security settings.

Check whether the account was used to send malicious emails.

- Determine whether other accounts may have been affected.

Management should:

- Consider whether customer or learner information may have been accessed.
- Consider whether a personal data breach has occurred.
- Determine whether affected customers need to be informed.

10. Ransomware or Malware

If ransomware or significant malware is suspected:

Do not attempt to resolve the incident independently.

The affected user should:

- Stop using the affected device.
- Disconnect it from the network if safe to do so and/or as directed by IT support.
- Do not delete ransomware messages or files.
- Do not attempt to pay or negotiate with attackers.
- Contact IT support immediately.

IT support should:

- Isolate affected devices/accounts.
- Determine the apparent scope.
- Protect unaffected systems.
- Prevent further spread.
- Preserve relevant evidence.
- Escalate to external cyber specialists where required.
- Establish whether backups are available and unaffected.
- Only begin restoration once the environment is considered sufficiently secure.

The Incident Lead should activate the Business Continuity Plan if critical business services are affected.

-
-
-
-

11. Suspected Data Breach

A personal data breach may involve:

- Unauthorised access.
- Unauthorised disclosure.
- Loss.
- Destruction.
- Alteration.
- Accidental transmission to the wrong recipient.

Examples relevant to the organisation include:

- Learner information sent to the wrong customer.
- Examination papers or learner records accessed without authorisation.
- A compromised employee mailbox containing learner/customer information.
- Personal information uploaded to the wrong SharePoint location.
- Lost equipment containing accessible personal information.

All suspected personal data breaches must be reported immediately to the designated management/data protection responsible person.

Do not wait until the full extent of the breach is known before reporting it internally.

Management should assess:

- What information is involved.
- Whose information is involved.
- How many individuals may be affected.
- Whether the information was actually accessed.
- Potential consequences for affected individuals.
- Whether containment has been achieved.
- Whether notification to the Information Commissioner's Office (ICO) is required.
- Whether affected individuals need to be informed.
- Whether customers or contractual partners need to be notified.

Where a personal data breach is reportable to the ICO, the organisation must normally notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it.

The 72-hour requirement should **not** be interpreted as allowing staff to delay internal reporting.

-
-
-
-

12. Loss of Microsoft 365

If Microsoft 365 becomes unavailable, the Incident Lead should determine whether the issue is:

- An organisation-wide Microsoft service outage.
- An account/access problem.
- A connectivity problem.
- A cyber security incident.
- A deliberate security restriction.

If the cause is unknown, the incident should initially be treated cautiously.

The organisation will maintain an emergency contact list that is available independently of Microsoft 365.

Where Microsoft 365 is unavailable:

Customer communications

Use any agreed alternative communication method.

Training delivery

Determine which scheduled courses are affected.

For online courses:

- Assess whether Teams can be restored.
- If not, determine whether an approved alternative platform is available.
- If no suitable platform is available, reschedule the course.

For face-to-face courses:

- Continue where trainers have the necessary information and materials.
- Use alternative communication arrangements to confirm attendance and arrangements.

Records

Avoid creating unnecessary duplicate records.

Once systems are restored, update official records and document any decisions made during the outage.

-
-
-
-

13. SharePoint Incident

If files appear to have been deleted, altered or encrypted:

- Do not continue making unnecessary changes to affected folders.
- Contact IT support.
- Identify the affected files/folders.
- Establish whether the issue is accidental deletion, synchronisation, malicious activity or another cause.
- Preserve evidence where possible.

-

Determine whether recovery from appropriate backup/version history is possible.

Restoration should be controlled to avoid overwriting useful evidence or spreading malicious changes.

14. Xero Incident

If unauthorised access to Xero is suspected:

- Report immediately to management and IT support.
- Secure the account.
- Review suspicious activity.
- Review changes to bank/payment information.
- Check recent transactions and invoices.
- Contact the appropriate support provider where necessary.
- Contact the bank immediately if fraudulent payment activity is suspected.

Financial transactions should be independently verified during a suspected account compromise.

15. Website or Online Booking Incident

If the website is compromised or unavailable:

- Notify the website/hosting provider as appropriate.
- Do not attempt unapproved technical changes.
- Determine whether customer booking information may have been exposed.
- Consider temporarily disabling affected functions if necessary.
- Establish an alternative method for customer enquiries and bookings.
- Maintain a record of manual bookings until normal systems are restored.

16. Customer and Learner Communications

Communication should be:

- Accurate.
- Timely.
- Proportionate.
- Consistent.
- Approved by the Incident Lead.

Staff should not speculate about:

- The cause of an incident.
The extent of a breach.

- Whether customer data was accessed.
- Whether the incident was caused by a particular person or organisation.

A basic communication should explain:

1. That an incident has occurred, where appropriate.
2. Whether the customer's course/service is affected.
3. What action is being taken.
4. What the customer needs to do.
5. When further information will be provided.

17. Business Continuity Activation

The Business Continuity process should be activated where the cyber incident is likely to:

- Prevent delivery of scheduled training.
- Prevent access to critical customer information.
- Prevent access to essential training materials.
- Prevent communication with customers/trainers.
- Affect multiple employees.
- Affect Microsoft 365 or other critical systems for a prolonged period.
- Cause significant loss of data.
- Require alternative working arrangements.
- Create significant regulatory, contractual or reputational risk.

The Incident Lead should document the decision to activate or not activate the BCP.

18. Maintaining Training Delivery

Where a cyber incident affects normal systems, the organisation should prioritise:

First priority

Training already scheduled within the next 24 hours.

Second priority

Courses scheduled within the following 48–72 hours.

Third priority

Future courses and routine administration.

For each affected course, determine:

- Customer.

-
- Course.
- Date/time.
- Trainer.
- Delivery method.
- Learner numbers.
- Required equipment.
- Required training materials.
- Whether delivery can continue.
- Whether it can move online.
- Whether another trainer can deliver it.
- Whether it needs to be rescheduled.

19. Evidence and Incident Records

The Incident Lead should maintain an incident log containing:

- Date/time incident identified.
- Person reporting incident.
- Description of incident.
- Systems affected.
- Initial severity.
- Actions taken.
- People notified.
- Decisions made.
- Customer impact.
- Data protection considerations.
- External organisations contacted.
- Recovery actions.
- Time systems were restored.
- Lessons identified.

Relevant emails, alerts, screenshots, logs and other evidence should be retained where appropriate.

Staff should not alter or delete potentially relevant evidence unless instructed.

20. Recovery

Systems should only be returned to normal operation once the Incident Lead and IT support are satisfied that it is appropriate to do so.

Recovery should include:

- Confirming the cause or likely cause where possible.
- Confirming affected accounts/devices have been secured.
- Restoring systems from trusted sources where necessary.
- Checking restored data.
- Resetting credentials where appropriate.
- Confirming security controls are functioning.
- Monitoring systems following restoration.
- Confirming critical business processes can resume.

21. Return to Business as Usual

The Incident Lead should formally stand down the incident when:

- Critical systems have been restored or acceptable alternatives established.
- Immediate security risks have been contained.
- Critical training delivery has resumed.
- Customer communications have been completed.
- Data protection actions have been completed or transferred to ongoing management.
- Outstanding recovery actions have owners.

A record should be made of the stand-down decision.

22. Post-Incident Review

A review should take place following:

- All Level 3 and Level 4 incidents.
- Significant data breaches.
- Significant ransomware/malware incidents.
- Major system outages.
- Any incident that resulted in cancelled or substantially disrupted training.
- Any incident where the BCP was activated.

The review should consider:

1. What happened?
2. When was it detected?

3. How effective was the response?
4. What worked well?
5. What did not work?
6. Was communication effective?
7. Were customers appropriately supported?
8. Was the Business Continuity Plan effective?
9. Were recovery objectives achieved?
10. What controls need strengthening?
11. What training is required?
12. What changes should be made to the BCP?

Actions should be assigned to named owners with target dates.

23. Cyber Incident Contact List

The following information must be completed and kept both electronically and in an accessible offline format.

Contact	Name	Telephone
Incident Lead	Emma Merrick	07834 731914
Deputy Incident Lead	Becca Lander	07518 906136
IT Support	Joe Foden	07926 461987

24. Preventative Controls

The following controls will be implemented.

Account security

- Multi-factor authentication should be enabled for Microsoft 365 and other critical systems where available.
- Unique passwords should be used.
- Passwords must not be shared.
- Access should be removed promptly when staff leave.
- Administrative accounts should be appropriately protected.

Email security

- Staff should receive regular phishing awareness training.
- Suspicious messages should be reported.
- Staff should verify unexpected payment or sensitive-information requests through an alternative communication channel.

Devices

- Business devices should use appropriate security controls.

- Devices should be kept up to date.
- Screen locking should be enabled.
- Lost or stolen devices must be reported immediately.

Data

- Access to SharePoint should be based on business need.
- Sensitive information should not be unnecessarily downloaded or copied.
- Critical information should have an appropriate recovery mechanism independent of the primary live environment.

Suppliers

A1 Education & Training will maintain appropriate security and continuity information for critical IT suppliers.

25. Testing

A1 Education & Training will test this procedure at least annually.

Testing will include scenarios such as:

Exercise 1 – Phishing

A trainer accidentally clicks a malicious link in an email.

Exercise 2 – Microsoft 365 compromise

An employee's Microsoft 365 account is suspected of being compromised.

Exercise 3 – Ransomware

Several files in SharePoint appear to have been encrypted or deleted.

Exercise 4 – Major outage

Microsoft 365 is unavailable during a day when several online courses are scheduled.

Exercise 5 – Data breach

Learner information is accidentally sent to the wrong customer.

Following each exercise, lessons will be recorded and improvements incorporated into the relevant procedures.

26. Employee Quick Reference

If you suspect a cyber incident:

STOP → DISCONNECT IF APPROPRIATE → REPORT → PRESERVE → FOLLOW INSTRUCTIONS

Do

- Report immediately.
- Tell IT support what happened.
- Preserve suspicious emails and information.
- Follow instructions.
- Record important details.

Don't

- Ignore the incident.
- Delete suspicious emails.
- Continue clicking links.
- Attempt to investigate independently.
- Share incident details externally.
- Attempt to negotiate with attackers.
- Assume someone else has already reported it.

27. Supporting documents

This procedure forms part of the organisation's Business Continuity Plan and should be read alongside:

- **Business Continuity Policy**
- **Business Continuity Analysis and Risk Assessment**
- **Major Incident Management Procedure**
- **Training Equipment inventory**
- **Business Continuity and Incident Log**

APPENDIX 4



Training Equipment Inventory

CONTENTS

1. Purpose
2. Equipment Register
3. Trainer Equipment Allocation
4. Equipment Continuity Requirements
5. Loss, Damage or Failure Procedure

6. Equipment Inspection and Maintenance
7. First Aid Equipment
8. Equipment Storage
9. Equipment Transportation
10. Equipment Loss or Theft
11. Equipment Replacement
12. Equipment Checks
13. Equipment Continuity Checklist
14. Equipment Register Responsibilities
15. Supporting Documents

1. Purpose

This register provides a central record of training equipment required to deliver the organisation's courses.

It supports business continuity by identifying:

- Equipment required for critical training.
- Equipment held by individual trainers.
- Equipment stored at the head office.
- Equipment that is essential to course delivery.
- Equipment that can be substituted.
- Equipment that requires replacement if lost or damaged.
- Equipment requiring inspection, maintenance or calibration.
- Equipment that may create a business continuity risk if unavailable.

The register should be maintained alongside the Business Continuity Risk Assessment and Business Continuity Plan.

2. Equipment Register

Equipment will be classified according to its importance to training delivery.

Classification	Definition	Example
Critical	Course cannot be delivered safely/appropriately without it	Required first aid training equipment
Important	Delivery is significantly affected but an alternative may exist	Projector
Standard	Useful but alternative arrangements are readily available	Additional presentation equipment
Non-critical	No significant continuity impact	Spare/general equipment

Asset ID	Equipment	Course/use	Quantity	Location/help by	Condition	Critical?	Inspection/ expiry	Replacement available?	Action if unavailable
EQ-001									
EQ-002									
EQ-003									
EQ-004									
EQ-005									
EQ-006									

3. Trainer Equipment Allocation

Because trainers generally retain their own equipment, the organisation will maintain a record of who holds critical equipment.

Trainer	Equipment/ kit	Asset ID	Quantity	Condition	Last checked	Replacement required?
Trainer 1						
Trainer 2						
Trainer 3						
Trainer 4						
Trainer 5						
Trainer 6						
Trainer 7						
Trainer 8						
Trainer 9						
Trainer 10						

4. Equipment Continuity Requirements

For each item identified as **Critical**, the organisation will establish:

- Who normally holds the equipment.
 - Whether a spare is available.
 - Whether another trainer has suitable equipment.
 - Whether equipment can be hired or purchased quickly.
 - Whether the customer has suitable equipment.
 - Whether the course can be delivered at another venue.
 - Whether the course can be rescheduled.
 - Whether the course can be delivered online.
-

5. Loss, Damage or Failure Procedure

If critical equipment is lost, stolen, damaged or becomes unusable:

Step 1 – Report

The trainer should notify the Head of Quality or Company Director as soon as possible.

Step 2 – Assess Determine:

- What equipment is affected?
- Which course is affected?
- When is the course scheduled?
- Is the equipment essential?
- Is a replacement available?
- Can another trainer provide equipment? [Step 3 – Identify alternative](#)

Consider:

13. Spare organisational equipment.
14. Equipment held by another trainer.
15. Hire or purchase of replacement equipment.
16. Customer-provided equipment, where appropriate and suitable.
17. Alternative venue.
18. Alternative trainer.
19. Online delivery, where appropriate.
20. Rescheduling.

Step 4 – Record

The incident should be recorded where the loss or failure is likely to affect business continuity, customer delivery, safety or compliance.

6. Equipment Inspection and Maintenance

Equipment owners are responsible for ensuring that equipment allocated to them is:

- Present and available.
- Suitable for its intended use.
- Clean and appropriately stored.
- In a serviceable condition.
- Within any applicable expiry or inspection period.
- Transported safely.
- Reported if damaged or missing.

Where equipment has a manufacturer's recommended inspection, servicing or replacement interval, this should be recorded.

Where equipment is used for regulated or accredited training, any applicable awarding body or manufacturer requirements should also be followed.

7. First Aid Equipment

First aid training equipment should receive particular attention because practical equipment is fundamental to the delivery of many first aid courses.

The organisation will maintain sufficient equipment to support scheduled courses and have a contingency arrangement for:

- Damaged equipment.
- Missing equipment.
- Equipment failure.
- Expired consumables.
- Trainer absence.
- Last-minute additional course requirements.

Consumable items will be monitored to prevent shortages.

8. Equipment Storage

Equipment held by trainers should be stored securely and protected from:

- Theft.
- Damage.
- Excessive heat/cold.
- Moisture.
- Unauthorised use.
- Loss during transportation.

Trainers should not leave valuable or critical equipment unattended in vehicles for prolonged periods where this creates an avoidable theft risk.

9. Equipment Transportation

Before travelling to a customer venue, the trainer should confirm:

- Required equipment is available.
- Equipment is in suitable condition.
- Any required consumables are available.
- Equipment can be safely transported.
- The equipment required for the specific course matches the course requirements.

Where equipment is particularly critical, the trainer should identify any contingency arrangement before leaving for the venue.

10. Equipment Loss or Theft

Lost or stolen equipment must be reported promptly.

The organisation should determine:

- Whether the equipment is organisation-owned.
- Whether personal information is associated with the equipment.
- Whether the loss affects an imminent course.
- Whether insurance notification is required.
- Whether replacement is required.
- Whether the incident needs to be recorded under the Business Continuity Plan.

If the equipment contains business or personal information, the **Cyber Incident Procedure/Data Breach Procedure** must also be considered.

11. Equipment Replacement

For critical equipment, management determine the following reasonable replacement timescale.

Equipment category	Target replacement
Critical first aid equipment	As soon as practicable / before affected course
Essential course materials	Within 24 hours where possible
Important practical equipment	Within 48–72 hours where possible
Standard equipment	Within 5 working days where required

12. Equipment Checks

A formal equipment review will be completed:

- At least annually.
- When a new course is introduced.
- When equipment is replaced.
- Following equipment loss or damage.
- Following a continuity incident.
- Following a customer complaint relating to equipment.
- Before significant periods of increased training activity.

The review should confirm:

- Equipment inventory is accurate.
- Equipment holders are correctly recorded.
- Equipment remains suitable.
- Critical equipment has a contingency.
- Expired equipment has been replaced.
- Required inspections have been completed.

13. Equipment Continuity Checklist

Before a course

- ☐ Confirm course requirements.
- ☐ Confirm required equipment.
- ☐ Confirm equipment is available.
- ☐ Check equipment condition.
- ☐ Check consumables.
- ☐ Check any relevant expiry/inspection dates.
- ☐ Confirm equipment can be transported safely.
- ☐ Identify contingency arrangements for critical equipment.

If equipment becomes unavailable

- ☐ Notify Training/Operations Lead.
- ☐ Identify the affected course.
- ☐ Assess whether equipment is essential.
- ☐ Check whether another trainer has suitable equipment.
- ☐ Check availability of spare equipment.
- ☐ Consider hire/purchase.
- ☐ Consider alternative venue.
- ☐ Consider alternative trainer.
- ☐ Consider online delivery if appropriate.
- ☐ Consider rescheduling.
- ☐ Record the incident where appropriate.

14. Equipment Register Responsibilities

Quality Lead

Responsible for:

- Maintaining the master equipment register.
- Identifying critical equipment.

- Monitoring equipment continuity risks.
- Coordinating replacement.
- Reviewing equipment availability.

Individual Trainers

Responsible for:

- Looking after equipment in their possession.
- Reporting damage, loss or theft.
- Ensuring equipment is suitable before use.
- Reporting shortages or expiry issues.
- Keeping the organisation informed of significant changes to equipment held.

Management

Responsible for:

- Providing appropriate resources.
- Approving replacement of significant/critical equipment.
- Ensuring equipment risks are incorporated into the Business Continuity Risk Assessment.

15. Supporting Documents

- **Business Continuity Policy**
- **Business Continuity Analysis and Risk Assessment**
- **Major Incident Procedure**
- **Cyber Incident Procedure**
- **Business Continuity and Incident Log**

APPENDIX 5



Business Continuity and Incident Log

CONTENTS

1. Purpose
2. Incident Details
3. Incident Type
4. Initial Incident Description
5. Immediate Safety Assessment
6. Initial Business Impact Assessment
7. Affected Training
8. Initial Risk Assessment
9. Incident Escalation
10. Chronological Incident Record
11. Key Decisions
12. Customer Communications
13. Staff/Trainer Communications
14. Data Protection Assessment
15. Cyber/IT Incident Record
16. Business Continuity Actions
17. Recovery record
18. Stand-Down Assessment
19. Incident Closure
20. Post-Incident Review
21. Lessons Learned and Corrective Actions
22. Evidence and Supporting Information
23. Incident Log Completion Checklist

24. Supporting documents

1. Purpose

This Incident Log is used to record significant incidents affecting, or potentially affecting, the organisation's people, customers, learners, training delivery, premises, information, IT systems or business operations.

It provides a chronological record of:

- What happened.
- When it happened.
- Who was involved.
- Actions taken.
- Decisions made.
- Communications issued.
- Business impact.
- Recovery activities.
- Outstanding actions.

The log may also provide an important record for subsequent investigation, insurance, customer assurance, regulatory requirements and lessons learned.

2. Incident Details

Field	Information
Incident reference	
Date incident identified	
Time incident identified	
Date/time incident started, if known	
Reported by	
Contact details	
Incident Lead	
Deputy Incident Lead	
Incident type	
Initial severity	Level 1 / 2 / 3 / 4
BCP activated?	Yes / No
Date/time BCP activated	
Date/time incident closed	

3. Incident Type

Tick all that apply:

- ☐ Cyber/security incident
 - ☐ Data/personal information incident
 - ☐ IT/system failure
 - ☐ Microsoft 365 outage
 - ☐ SharePoint/data access issue
 - ☐ Xero/financial system incident
 - ☐ Website/booking system incident
 - ☐ Loss of premises
 - ☐ Fire
 - ☐ Severe weather
 - ☐ Transport disruption
 - ☐ Staff/trainer shortage
 - ☐ Customer venue disruption
 - ☐ Training equipment loss/failure
 - ☐ Supplier failure
 - ☐ Health and safety incident
 - ☐ Serious injury/illness
 - ☐ Reputational incident
 - ☐ Other: _____
-

4. Initial Incident Description

Provide a factual description of what happened.

Include:

- What happened?
- When did it happen?
- Where did it happen?
- How was it identified?
- Who identified it?
- What is known about the cause?
- What is not yet known?

Description:

5. Immediate Safety Assessment

Question	Response
Is anyone in immediate danger?	
Has anyone been injured?	
Are emergency services required?	
Has the affected area been made safe?	
Are staff/trainers safe?	
Are customers/learners safe?	
Further action required?	

If emergency services are required, this must not be delayed while completing this form.

6. Initial Business Impact Assessment

Area	Impact	Details
Employees	None / Low / Medium / High / Critical	
Trainers	None / Low / Medium / High / Critical	
Customers	None / Low / Medium / High / Critical	
Learners	None / Low / Medium / High / Critical	
Training delivery	None / Low / Medium / High / Critical	
Head office	None / Low / Medium / High / Critical	
Microsoft 365	None / Low / Medium / High / Critical	
Outlook/email	None / Low / Medium / High / Critical	
Teams	None / Low / Medium / High / Critical	
SharePoint	None / Low / Medium / High / Critical	
Xero	None / Low / Medium / High / Critical	

Website/booking	None / Low / Medium / High / Critical	
Training equipment	None / Low / Medium / High / Critical	
Business information	None / Low / Medium / High / Critical	
Personal data	None / Low / Medium / High / Critical	
Financial operations	None / Low / Medium / High / Critical	
Reputation	None / Low / Medium / High / Critical	

7. Affected Training

Complete where the incident affects course delivery.

Course	Customer	Date/time	Trainer	Delivery method	Status	Action

Status

Green: Continue as planned.

Amber: Continue with changes.

Red: Unable to continue; alternative arrangement required.

8. Initial Risk Assessment

Risk	Likelihood	Impact	Rating	Immediate control

9. Incident Escalation

Time	Person/role notified	Method	Information provided	Response

People/organisations that may need to be contacted include:

- Incident Lead.
- Senior Management.
- IT Support.
- External IT/Cyber Support.
- Data Protection Lead.
- Insurance provider.
- Customer(s).
- Awarding/accreditation body.
- Relevant supplier.
- Relevant authority/regulator.
- Emergency services.

Only contacts relevant to the incident should be notified.

10. Chronological Incident Record

Record significant actions, events and decisions in chronological order.

Date	Time	Action/event/decision	Person responsible	Outcome/follow up

11. Key Decisions

Important management decisions should be recorded separately.

Date/time	Decision	Reason	Decision maker	Action required

Examples include:

- Activating the Business Continuity Plan.
- Cancelling or rescheduling training.
- Moving training online.
- Closing the head office.
- Changing communication arrangements.
- Isolating IT systems.
- Notifying customers.
- Contacting insurers.
- Reporting a data breach.
- Restoring systems.
- Standing down the incident response.

12. Customer Communications

Date/time	Customer	Method	Person communicating	Summary	Follow-up

13. Staff/Trainer Communications

Date/time	Audience	Method	Person communicating	Summary

14. Data Protection Assessment

Complete if the incident involves, or may involve, personal information.

Question	Response
Does the incident involve personal data?	Yes / No / Unknown
What type of information may be affected?	
Whose information may be affected?	
How many individuals may be affected?	
Has information been lost?	
Has information been disclosed?	
Has unauthorised access occurred or potentially occurred?	
Has the incident been contained?	
Data Protection Lead notified?	
Date/time notified	
ICO notification considered?	
Customer notification considered?	
Individual notification considered?	
Question	Response
Further action required	

Important: Suspected personal data incidents should be escalated promptly and should not be delayed while the full extent of the incident is established.

15. Cyber/IT Incident Record

Complete where appropriate.

Item	Details
System affected	
User/account affected	
Device affected	
Date/time detected	
Date/time access stopped/contained	
IT Support notified	
External IT/Cyber support notified	
Account secured	
Device isolated	
Evidence preserved	
Backups/recovery considered	
Systems restored	
Additional monitoring required	

16. Business Continuity Actions

Action	Owner	Priority	Target completion	Completed	Date
		High/Med/Low			
		High/Med/Low			
		High/Med/Low			
		High/Med/Low			
		High/Med/Low			

17. Recovery Record

Service/system	Problem	Recovery action	Restored date/time	Verified by
Microsoft 365				
Service/system	Problem	Recovery action	Restored date/time	Verified by

Outlook				
Teams				
SharePoint				
Xero				
Website/booking				
Training delivery				
Other				

18. Stand-Down Assessment

Before closing the incident, confirm:

- ☐ Immediate safety risks have been controlled.
- ☐ Emergency services involvement has ended or been transferred.
- ☐ Critical training has resumed or alternative arrangements are in place.
- ☐ Affected customers have been informed.
- ☐ Staff/trainers have been informed as appropriate.
- ☐ Critical IT systems have been restored or alternatives established.
- ☐ Data protection implications have been assessed.
- ☐ Insurance requirements have been considered.
- ☐ Outstanding actions have been assigned.
- ☐ Temporary arrangements have been documented.
- ☐ Incident Lead considers the organisation ready to stand down.

19. Incident Closure

Incident stand-down date: _____

Incident stand-down time: _____ Incident

Lead: _____ Reason for
closure:

Outstanding actions transferred to:

20. Post-Incident Review

A review should normally be completed following a Level 3 or Level 4 incident and may be completed following a Level 1 or Level 2 incident where useful.

What happened?

What went well?

What did not go well?

Were customers affected?

Were learners affected?

Was training cancelled or disrupted?

Were recovery objectives achieved?

Were there any data protection concerns?

Were the Business Continuity Plan and procedures effective?

What should be changed?

21. Lessons Learned and Corrective Actions

Issue/lesson	Corrective action	Owner	Priority	Target date	Completed
			High/Med/Low		
			High/Med/Low		

			High/Med/ Low		
			High/Med/Lo w		

Corrective actions should be incorporated into the relevant:

- Risk assessment.
- Business Continuity Plan.
- Cyber Incident Procedure.
- Major Incident Procedure.
- Training Equipment Register.
- IT arrangements.
- Staff training.
- Supplier arrangements.

22. Evidence and Supporting Information

Record the location of relevant evidence.

Evidence	Location/reference	Person responsible
Emails		
Screenshots		
IT logs		
Customer communications		
Photographs		
Supplier correspondence		
Insurance correspondence		
Other		

Evidence relating to a cyber incident or potential data breach must be retained securely and must not be unnecessarily altered or deleted.

23. Incident Log Completion Checklist

- ☐ Incident reference allocated.
- ☐ Initial incident details recorded.
- ☐ Severity assessed.

- ☐ Immediate safety assessed.
- ☐ Business impact assessed.
- ☐ Incident Lead appointed.
- ☐ Relevant personnel notified.
- ☐ BCP activation considered.
- ☐ Affected training identified.
- ☐ Customer impact assessed.
- ☐ Data protection implications considered.
- ☐ IT/cyber implications considered.
- ☐ Key decisions recorded.
- ☐ Actions assigned.
- ☐ Recovery recorded.
- ☐ Stand-down authorised.
- ☐ Post-incident review completed where required.
- ☐ Corrective actions assigned.
- ☐ Risk assessment reviewed/updated where necessary.
- ☐ Incident record securely stored.

24. Supporting Documents

- 1. Business Continuity Policy**
- 2. Business Continuity Analysis and Risk Assessment**
- 3. Major Incident Procedure**
- 4. Cyber Incident Procedure**
- 5. Training Equipment Inventory**