Business Continuity Policy

Orangebox Training

Contents

Policy Statement

The Civil Contingencies Act 2004 requires Orangebox 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.

Orangebox's Business Continuity Policy shall be implemented in all departments and locations where Orangebox has an office or employees.

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

Assumptions used to support Orangebox's planning process include the following elements.

- Emergencies or threatened emergencies can adversely impact Orangebox's ability to continue to support critical activities and provide support to the operations of learners, employers, partners and external agencies.
- When a business continuity event is declared, Orangebox 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, learners, employers, partners and local agencies to function with limited automated support and some degradation of service, until full recovery is made.

Orangebox 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, Orangebox is undertaking a continuous programme of work to prepare a revised 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.

Orangebox Business Continuity Plan aims to:

- Prioritise people's safety
- Maintain essential services
- Protect buildings and their contents and sensitive information.

The following three generic types of scenarios are suggested as likely to trigger BCP activation:

Orangebox 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 Orangebox 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 in order 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 of Orangebox and 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 Orangebox or loss of reputation.
- Priority 3 - Activities that do not fall into either of the first two categories.

Regular review of the continuity requirements and plans to ensure that they reflect the needs of the business

Each service should assure itself that its key suppliers or partners which support a critical activity have effective BCM arrangements in place.

Orangebox 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 Chief Executive Officer has, overall, responsibility for ensuring that the management of business continuity is incorporated in Orangebox's processes and structure. Senior Management Team are responsible for ensuring that all services comply with this policy.

Contract Specific Continuity Risks

Delivery

Contract Volume Changes

Risk: Orangebox has prepared to deliver the volumes set out in the initial contract. There is a risk that these volumes will suddenly increase, leading to the need for the rapid deployment of additional resource to cope with this increase.

Solution: Orangebox has access to qualified and trained staff in the relevant area. We also have access to a number of subcontractors and potential subcontractors. In the event that we are notified of a likely increase in volume, we will:

- Draft in staff from other contracts where this is feasible; and/or
- Instigate our capacity identification communication process to identify the most appropriate subcontractor with available resource

Likelihood of occurrence: medium

Impact of occurrence: low/medium

Subcontractor Failure

Risk: Orangebox will, where necessary, use subcontractor organisations to ensure that both the range and volume of customer needs can be met at all times. The selection of subcontractors will be important to ensure that a stable, flexible and varied supply chain is established. Given the current economic climate there is however a risk that a subcontracting organisation could experience performance difficulties and even insolvency, thereby leaving them unable to deliver on this contract.

Solution: Orangebox has put in place a rigorous system of subcontractor selection which investigates the financial status as well as the performance history of the subcontractor.

Financial Failure Measure

- Where a supplier is deemed to be necessary to the contract due to a specialism but has an insufficiently robust track record (for example because they are a relatively new organisation), the volumes allocated to such an organisation will be reduced and only increased on proof of performance.
- Wherever possible two contractors offering similar provision will be identified. Where necessary a ‘waiting list’ of subcontracting organisations will be held to ensure rapid access to pre-validated subcontractors is available.

Likelihood of occurrence: medium

Impact of occurrence: low to high dependant on contractor size

Performance Failure Measures

- A rigorous performance management system is in place in order to ensure "early warning" of performance issues. This gives Orangebox the platform to put in place remedial actions to bring the subcontractor up to standard quickly. Where relatively new subcontracting organisations are recruited, our capacity building strategy, which includes more frequent interventions and support, will be put in place.

- Wherever volumes allow two subcontracting organisations with a similar specialism will be recruited. Where projected volumes mean this approach represents poor value for money, or is unviable, every effort will be made to have a second potential provider on our "standby" or waiting list. These providers will be pre-validated in terms of their financial robustness and track record wherever possible.

Likelihood of occurrence: low to medium

Impact of occurrence: low to medium

Loss of Delivery Centre

Risk: There is a risk that a disaster could render the centre from which Orangebox delivers unusable.

Solution: In such a situation, Orangebox would divert delivery of services to either another office located at the site or another site where secure login can be confirmed. Incident offices have good physical security, are operating to ISO27001 standards and have ample working and meeting space. Either would be used while suitable replacement facilities were constructed.

Likelihood of occurrence: low

Impact of occurrence: medium

Safeguarding

Risk: The programme will involve Orangebox working with a high number of vulnerable adults and or young people. Whilst there are stringent safeguarding systems in place, there is a risk that a customer may be put at risk or harmed by a member of staff or another customer whilst on the programme.

Solution: Orangebox has robust and stringent safeguarding policy and procedures, which it publicises to all members of staff. Prior to the employment of any member of staff, DBS checks at the relevant level for the position applied for are performed, and any risk identified from these are dealt with appropriately. In order to ensure that our subcontractors have the same rigour we insist on the following:

- All staff to be DBS checked at the level appropriate to their role and to have received safeguarding training with appropriate records being kept to demonstrate this.

- Incident logs to be kept and any incidents, however minor, to be reported to the Orangebox Designated Safeguarding officer.

In the unlikely event that an incident does occur the following investigation procedure will be followed:

- The details of the incident and those alleged to have been involved will be ascertained by DSL or DDSL.

- The members of staff alleged to have been involved will be suspended on full pay until the incident has been fully investigated and an outcome reached.

- Where appropriate the relevant authorities (LSPs, Social Services, Police, relevant contract funder) will be informed and advice sought.

- Should the complaint involve allegations of criminal activity, the Police will be contacted for support or to investigate as they see appropriate.

- The outcome of the investigation will be fully evaluated and any necessary remedial action will be taken in accordance with the disciplinary procedures of Orangebox or the subcontractor involved.

- Any and each incident of a safeguarding nature will result in a review of safeguarding policy and procedures in order to prevent future incidents. The relevant contract funder and where necessary the DBS will be kept informed of any action taken, in line with company policy.

Likelihood of an occurrence: low

Impact of an occurrence: high

Contract Risks

Contract Transition

Risk: When taking over a contract from the previous contract holder there is a risk that employers or learners currently on the programme will become lost in the handover process. Neither of these occurrences is acceptable as both will lead to customer/employer hardship and a drop, in contract performance.

Solution: Orangebox staff has experience of the transfer of customers across contracts and has a robust system in place to ensure that effective communications between providers takes place. This system will be implemented on notification of contract award.

Involving subcontractors in the process will be critical. The following process will be followed:

Ensuring the subcontractor is fully involved in the transition strategy will be a key critical success factor in the seamless handover of customers on the programme. Their involvement will vary but will include the following:

- **Transition Task Force**: for larger subcontractors, we will invite them to participate in the task force. They will advise and challenge the strategy from a subcontractor view.
- **Dedicated Lead**: subcontractors will nominate a transition lead within their organisation. They will be responsible for attending any meetings as part of the overall strategy and disseminating information within their organisation.
- **Communication Plan**: we will develop an effective plan to be used across the subcontractors, including suggested communication with key stakeholders.
- **Employer Engagement**: employers with learners understand the changes and the support they will receive.

The same process will be followed in the unlikely event of Orangebox being unable to carry on delivering to employers and learners. This will ensure the learners, employers, staff and subcontractors are kept informed and can input into activities taking place with the new contract holder unless the new contract holder has their own procedures that differ significantly from Orangebox's and we will follow their specific procedures and communications with all involved. Orangebox will inform the relevant funder immediately of any circumstance that may negatively impact on our ability to deliver to the contractual requirements and will work with the relevant funder in transitioning learners, employers and all paperwork/data to the new provider/s.

Likelihood of an occurrence: low

Impact of an occurrence: low

Human Resources

Risk: Lack of capacity due to Chief Executive Officer being absent due to either long term sick or leaving the organisation.

Solution: Orangebox Senior Management Team would cover short term up to 2 weeks. For longer term absences, Orangebox would place the most suitable, qualified and competent member of the SMT into the role as an interim measure until the MD returns to work or a new member of staff is recruited and in post.

Likelihood of Occurrence: medium

Impact of Occurrence: high

Risk: Lack of capacity due to Orangebox Team members being absent due to either long term sick or leaving the organisation.

Solution: With regards to the Team, the Team are trained to cover each other, plus the MD could cover short term up to 2 weeks in which time a replacement (permanent or temporary) could be sourced.

Likelihood of Occurrence: low

Impact of Occurrence: medium

ICT Security

Risk: Unauthorised access to or printing from the PCs used to access the interim funders data.

Solution: The member of staff authorised to access the data will have an individual PC logon.

Complex passwords will be used and are as follows:

- Eight character minimum
- Alpha-numeric with at least one digit
- Changed every 90 days
- Not reused within five password changes
- They also cannot use any part of their username

Likelihood of occurrence: low

Impact of occurrence: medium

Training

Risk: All employees of the organisation and where relevant subcontractors and third-party users MUST receive appropriate awareness training and awareness updates in organisational policies and procedures as relevant for their job function.

Solution: There is a comprehensive training programme which includes information security, data protection and freedom of information which includes all the requirements of the GDPR.

In addition, the Orangebox senior management team meets on a monthly basis and discuss data protection and information security matters as part of MIS.

Risk: Employees of the organisation who handle information carrying a protective marking of "RESTRICTED" must be made aware of the impact of loss of such material and the actions to take in the event of any loss.

Solution: There is a security reporting process in place. This policy requires all employees to report any security incidents to the Data Controller within Orangebox. Our information security training includes a section on the protected marking scheme and responsibilities.

Likelihood of Occurrence: low

Impact of Occurrence: medium

ICT Outage

Risk: Loss of ICT and network services have a high level of impact on customer service and other areas of contract compliance.

Solution: Resumption of service at the earliest possible moment is key. Any ICT failure must be a priority (after person safety and data security). The process for ICT outage is as follows:

- Notify the Data Controller, who will contact Orangebox's network provider of outage to determine cause and timeframe for its recovery.
- If outage will be greater than four hours, route all calls via Directors/Managers and Quality Manager's mobiles.
- If data has become corrupt as part of the outage, advise the Data Controller of this at the earliest possible opportunity.
- The ICT support organisation will retrieve a clean version of the data from the latest backup.
- If no network provider outage is discovered, the Data Controller and ICT support organisation will investigate alternative reasons for the failure (e.g. cables being cut) and rectify accordingly.

Likelihood of an occurrence: low

Impact of an occurrence: medium

Data Security

Risk: Loss of data/data access. Access to data is a priority and the following procedures are to ensure that should any Orangebox's location be inaccessible, access to key data can still be obtained, allowing as normal a service as possible.

Solution: Data backup.

- Full and incremental backups preserve company information assets and should be performed on a regular basis for audit logs and files that are irreplaceable, have a high replacement cost, or are considered critical. Backup media should be stored in a secure, geographically separate location from the original and isolated from environmental hazards.

- Contract specific data and document retention (see Data and Information Security Policy) specify what records must be retained and for how long. All departments are accountable for carrying out the provisions of the instruction for records in their organisation.

Solution: Data backup and access.

- Orangebox's data is backed up hourly at Microsoft's Data Centres. The data held at the backup site can be accessed 24 hours per day, seven days per week, meaning swift retrieval in the event of a disaster occurring. The backup media storage facility is secure, isolated from environmental hazards and geographically separate from the location.

Likelihood of an occurrence: low

Impact of an occurrence: high

Solution: Telecommunications failure will not affect subcontractor communications. In the event of telecommunications failure lasting longer than 48 hours, Orangebox would divert delivery of services with our Managed Service Provider, Prism Solutions.

Likelihood of an occurrence: low

Impact of an occurrence: high

Paperwork sent via Postal Service

Risk: Confidential paperwork is posted by the subcontractor when there is no-one at Orangebox to receive it, e.g. Bank Holidays, Christmas Breaks. The confidential post is then left unattended at the office buildings security reception desk and therefore at risk of being lost or stolen.

Solution: The new process means the subcontractor is contacted before each Bank Holiday/Christmas Break and informed not to send any post to Orangebox until after the Bank Holiday, Christmas Break etc. is over.

Likelihood of an occurrence: Medium

Impact of an occurrence: Low

Risk: Postal Strike effect the delivery of Confidential paperwork between subcontractor and Orangebox

Solution: Orangebox would inform the subcontractor and implement a hand delivery system to ensure that there is no disruption to the service.

Likelihood of an occurrence: Low

Impact of an occurrence: Low

Natural Disasters

Risk: Natural disasters by their nature are unpredictable and can cause severe disruption to business delivery.

Solution: In the event of a major natural disaster affecting an Orangebox facility where notice is given, an emergency response process will be put in place. The process will be as follows:

- The first person aware should contact a member of the senior management team (SMT) who will then notify the rest of the team (or allocate someone to do so). Depending on the location and nature/scale of the event, a member of SMT may go to the location, or leave it to the location response coordinator (LRC) to attend. See appendix one for details of team members.

- In the event of a natural disaster of which there is advance notice, the following actions will be taken:
  - Notify Chief Operating Officer, of impending event, if time permits.

- If impending natural disaster can be tracked, begin preparation of alternate location within 72 hours as follows:
  - Contact Chief Executive Officer, to relocate to the alternate location.
  - Engage support personnel.
  - Contact insurance company.
  - Review all potential impacts and initiate action plans accordingly.

- 24 hours prior to event:
  - Create an image of the system and files.
  - Back up critical system elements.
  - Verify backup office is available from the alternate location.
  - Create backups of e-mail, file servers, etc.
  - Notify senior management.
  - Set up staff, partner and customer communications systems and draft messages.

Solution: In the event of a natural disaster of which there is no advance notice, the following actions will then be taken:

- Evacuate the building if appropriate.
- Contact the emergency services.
- Contact the Senior Management Team.
- Respond to the advice of the Senior Management Team regarding further actions.

Likelihood of an occurrence: low

Impact of an occurrence: high

Risk: Fire breaks out in an Orangebox facility. The first consideration in the event of a fire is to ensure the safety of all persons in the building and to ensure a proper evacuation procedure is followed where this is necessary.

Solution: The precise solution will be dependant of the nature and severity of the fire. On discovery of a fire in an Orangebox facility the person discovering it should make an assessment of the situation and take appropriate action as set out in Orangebox's emergency fire procedures. The following key actions will be taken to ensure safety of persons within the building and neighbouring buildings:

- If fire or smoke is present in the facility, the staff member who discovers it should evaluate the situation, determine the severity and take the appropriate action as defined in this section. Call the emergency services as soon as possible if the situation warrants it. If in any doubt, always evacuate and call 999.
- In the event of any emergency situation such as fire, personnel/customer/ visitor safety, followed by system and site security, are the major concerns. If in any doubt, the building should be evacuated using agreed procedures. This includes liaison with any other occupants of the building and alerting those in neighbouring buildings.
- If possible, the manager responsible for the site should remain present at (but at a safe distance from) the facility until the fire brigade has arrived. A staff roll-call should be taken and if possible, a rollcall of everyone using and visiting the building.
- Do not attempt to re-enter the building but wait for the emergency services to arrive and alert them to possible people still inside.

- Orangebox has fire wardens, whose instructions should be obeyed in the event of a fire. Only staff trained to use fire equipment are authorised to do so.

- Lifts are not to be used in the event of smoke or fire being discovered.

- In the event of a major catastrophe affecting the facility, immediately (after contacting the emergency services) notify a member of the SMT and the relevant director plus the manager if they are not already aware.

Likelihood of an occurrence: low

Impact of an occurrence: high

Pandemic or Infection Alert

- If any Orangebox location is affected by a mass illness such as a flu pandemic or a suspected infection (including any suspicion of terrorist or criminal-initiated infection such as an anthrax scare), then staff, customer and any other person's health and safety is the primary concern. Flu or other pandemic is likely to build up with increasing loss of staff for work so should be treated as an HR issue and alerted as soon as possible to the HR Advisor. The HR Advisor will consult with the SMT to see whether the office needs to be closed or to find additional support for the duration. If a flu or similar pandemic is confirmed, HR will liaise with government medical advisers and instruct accordingly.

- If a possible contamination of any kind threatening to health is suspected, procedures as for fire evacuation should be followed, with people instructed to gather at a central point and to remain in place until expert medical advice can be obtained. The most senior person present should contact HR, who will immediately obtain specialist government advice. The building should not be re-entered until it has been cleared by the emergency services, who will advise on/undertake any necessary decontamination procedures.

- The SMT will alert communications personnel and they, working with HR, will undertake communications with staff, families and local/national media as necessary. Everyone else should be reminded not to speak with the media unless authorised to do so.

Likelihood of an occurrence: low

Impact of an occurrence: high

Suspect Mail

Risk: Mail with a suspicious appearance may contain such threats to life or health as explosive devices or chemical agents such as anthrax.

Solution: Vigilance is required at all time, and in particular at times of a known terrorist threat. The following procedures should be applied to ensure proper attention is given to this threat at all times:

- Look out for suspicious envelopes or packages (such as discolouration, crystals, strange odours or oily stains, powder, excessive tape or string, unusual size or weight, lopsided or oddly-shaped envelope, postmark that does not match return address, excessive postage, handwritten, block-printed or poorly-typed addresses/title but no name, addressed to individual no longer with organisation).

- Open all mail with a letter opener.

- Do not blow into envelopes.
- Do not shake or pour out contents.
- Keep hands away from nose and mouth while opening mail.
- Wash hands after handling mail.
- If you are in any doubt about a package, do not touch it, move it or open it and call the police on 999.
- If you believe you have handled a contaminated package;
  - do not touch the package further or move it to another location
  - shut windows and doors in the room and leave the room, but keep yourself separate from others and available for medical examination
  - switch off any room air conditioning system
  - notify the building manager who should call 999 and close all fire doors and windows in the building.
- If there has been a suspected biological contamination, ensure that personnel outside the room are evacuated as soon as possible and ensure individuals in the contaminated room are evacuated to an adjacent unoccupied room away from the hazard.
- If you find a suspect package outside a building do not touch it or move it, instead inform the building manager clearly stating why you believe a biological/chemical material is involved
- If anyone believes they have been exposed to biological/chemical material, remain calm, do not touch eyes, nose or any other part of the body and wash your hands in ordinary soap where facilities are provided, but staff movement outside contained locations should be avoided as much as possible

Likelihood of an occurrence: low

Impact of an occurrence: medium

Flood or Water Damage

In the event of a flood or broken water pipe within any facilities, the guidelines and procedures in this section are to be followed.

Major Flood

- Assess the situation and determine if outside assistance is needed; if this is the case, dial 999 immediately and evacuate the facility.
- If water is originating from above electrical equipment, power down said equipment, provided it is safe to do so.
- Water detected may have different causes:
- If water is slowly dripping from an air-conditioning unit and not endangering equipment, contact repair personnel immediately.

- If water is of a major quantity and flooding beneath the floor (water mains break), immediately implement power-down procedures. While power-down procedures are in progress, evacuate the area and alert one of the emergency personnel.
- Provide them with your name, phone number where you can be reached, site and the nature of the emergency. Follow all instructions given.

Likelihood of an occurrence: low

Impact of an occurrence: medium

Auditing and Testing of the Business Continuity Plan

A regular auditing schedule has been put in place to ensure that the procedures outlined in this plan remain appropriate.

Desktop testing exercises will be carried out regularly.

Lead Responsibility

The Chief Executive Officer or a senior member of the management team is responsible for declaring a disaster and invoking the use of the business continuity plan. They are also responsible for communications during the disaster (to customers, funders – as applicable, subcontractors, Employers, Learners, staff, the media, etc.) and for declaring the disaster to be over. In circumstances where phone calls made to key contact personal are not answered, a text will also be sent saying “Emergency Orangebox, please respond. The Local Response Coordinator will support the dissemination of all communications with exception of those involving the media which must be dealt with by a senior member of the management team only.

Annual Schedule of BCP Desktop Audit

Planned Audit Date	Actual Audit Date	Responsibility	Actions/Changes
October 2018	04/10/18		None identified
April 2019	25/04/19		None identified
Oct 2019	10/10/19		Data Security section updated Job Titles updated
April 2020	30/07/20		None identified
Oct 2020			

Record of BCP Changes

BCP Update Date	Responsibility	Actions/Changes
10/10/19		Data Security section updated to reflect data back up at Microsoft’s Data Centres. MD job title changed to Chief Executive Officer.
30/07/20		Some formatting changes to document. Job Title changes. Removal of XXXX from Consistency Team

Appendix A: Business Continuity Contacts List

Senior Management Team (SMT):

Name	Role	Mobile Phone
	Chief Executive Officer	
	Director of Development & Innovation	
	Head of Operations	
	Head of Compliance & M.I.	
	Head of Quality and Safeguarding	

Appendix B: Local Response Coordinator (LRC)

Name	Location	Mobile Phone
	XXXX Office	
	XXXX Office	

Appendix C: IT Support Services

Name	Email	Contact Tel No.

Appendix D: Delivery Continuity Policy

Continuity of Training Policy

Purpose Statement

The purpose of this plan is to outline the continuity arrangements we have in place to safeguard our provision. The policy identifies reasonable measures in place to respond to and be able to mitigate business risks where there is a potential of significant damage to business operations.

Responsibility

Our Head of Operations is responsible for this policy and plan, it will be reviewed on an annual basis. All staff are responsible in adhering to this policy and plan.

Principles

The principles of this plan are to:

- Outline actions required in the event of an emergency or incidents which threatens to disrupt the normal working practices of our business
- Ensure limited or no disruption to provision in the event of an emergency or threat.

We consider that the threats most likely to affect the services we provide are:

- Loss of key staff – requiring change of communication
- Damage to main premises of business e.g. Fire
- Loss of critical systems – IT failure or breach of IT
- Telephone line failure
- Supply chain failure - consumables
- Supply chain failure - trainers
- Severe weather condition.

In some cases, these incidents can be due to natural-causes e.g. severe weather, while in other cases, equipment failure or human error or involvement may be the cause. They have the possibility of leading to the following loses, which are likely to have a major impact on our operations.

- Expertise
- Buildings
- Equipment
- Facilities
- Data
- Personnel

- Reputation
- Funding and or contracts.

General Steps

- As this plan is stored on a remote server, it is secure in the event of a localised system failure, disaster or emergency and may be accessed by any team member, who is able to connect to the internet.
- Telephone and e-mail contact details for team members and trainers are stored in the staff and managers' mobile telephones.
- The business has buildings, contents, business interruption and practice expenses insurance policies, to meet the cost of repairs and other overheads, where necessary.
- All data is backed up daily by back-up tape, which is stored off site. This is also supported by our IT company, who take a remote back-up, which is stored at their premises.

Staff

Every staff member must be aware of the evacuation and health and safety arrangements that will impact their working environment. Staff must ensure they report critical incident or concern to the lead of this policy immediately.

Staff will be made aware of this policy within their induction and reinforced within training and drills.

Consistency Team

The team responsible for managing serious incidents and supporting this plan are listed below.

Staff Name	Title	Area of responsibility	Phone number	Email
		ICT, Health and Safety, Buildings and Facilities Management		
		Employer relations and communication Funder/s communication Support with communication to field staff including Tutors Reputation of the company. Communication across both office sites in XXX and XXX		
		Personnel Safeguarding of all staff Ofsted		

Staff Name	Title	Area of responsibility	Phone number	Email
		Supporting XXXX with H and S		
		H and S of all staff H and S of Tutors Communication with Trainers Employer on site activity and communication to learners, staff and support with employer communication		
		Department of Education		
		Department of Education contact		

Short Term Incidents

Power failure, water failure, heating and or severe weather will often lead to short term impacts on daily operations. These incidents are managed by Head of Operations and key staff listed above.

Information to staff and stakeholders will be communicated by the Head of Operations to ensure each team has up to date information on the current situation. Where an incident prevents staff from accessing the head office, staff will be asked to stay home where possible to work from home until further notice.

We will aim to rectify any incident as soon as possible to ensure minimal disruption to the operations of the business.

Continuity Plan

Communication Channel	**Website:** Is externally managed allowing us to regularly update the site via a third party, ensuring updates regarding services are timely uploaded, communication channels such as change of personnel or phone numbers can also be updated. **Management team:** The Senior Management Team (SMT) have direct phone and email to support further communication lines. **Email failure:** IT systems will be rebooted, and email downtime will be monitored, where email is not available apprentices, suppliers, staff and employers can be contacted via phone. **Telephone line failure:** In addition to the landline telephone line, all company directors and delivery staff have business mobiles. These numbers are sent to all employers, delivery staff, and suppliers. Our telephone and internet supplier can redirect calls to the alternative numbers, so that we can continue to receive and make calls using our normal telephone number. If all our landlines fail, calls can be redirected to the Head of Operation's mobile. **Delivery team:** Where there are changes to our Tutors the Management Team can directly call or email the learners. The Tutors have the ability to provide learning interventions face to face and remotely, ensuring flexibility to meet the employer needs.
Modes of transport	The Delivery Team primary transport method is by car, however alternative transport by public transport such as rail and bus are available. Head office/central staff have multiple transport approach these being car, public transport and walking. We have localised staff to open and close the premises, they are able to reach the premises by foot in the event of severe weather. No delivery is carried out at our head office. We do not offer transport to learners or employers as part of the provision.
Alternative site of operations	The Head of Operations are responsible for procuring alternative accommodation. The Financial Director will support the procurement processes and identify facilities and equipment required. Office based staff will also be able to work from home with provided equipment until alternative site is made available.
Supply chain (consumables) preventive measures	Our supply chain provides us with paper, printing services, courier, and learning support material. For each of these we have alternative suppliers, from whom we can source the same standard of services. We also store reserve stocks in the event of low supplies.
Back-up of business-critical systems	We renew IT systems on a regular basis. All IT hardware is protected by antivirus and antimalware software, that automatically updates from the internet on a regular basis. We also employ firewalls to protect our systems from unauthorised access and malicious damage. Our operating systems automatically download and install upgrades to reduce system vulnerabilities. The server contains a third hard drive that carries out an incremental backup every day. Data from the database is backed up across the network from the server to the office computer every working day. We also operate a "cloud" backup system, that copies all
Back-up and restore of data	

	critical data to a remote site, which improves data security (there is no movement of physical media that could be lost, stolen or damaged). Data backups can be accessed on the server, the office computer and from the "cloud" backup. We have discussed the issue of catastrophic system failure with our provider and have been advised that the practice computer system can be reinstated within 24 hours.
Loss of key member of staff	Identify interchangeable staff: All members of staff should have team members who can perform their roles, even if it is in a reduced capacity. Identify the relevant person and support them in carrying out business-critical activities. Assess extent of loss: Identify whether the affected staff member's absence is likely to be temporary, longer-term, or permanent. Keep in mind this may be a difficult period for the staff member and / or their family. If the staff loss is temporary, support the member of staff who will be filling the gap until the absent member of staff returns. If the absence is long-term or permanent: ❍ Recruit temporary or full-time replacement - Follow the standard recruitment procedure to find a full-time, part-time or fixed-term contract (as appropriate) replacement to ensure smooth apprenticeship delivery.

Monitoring

Incidents that have trigged this policy are monitored to ensure there is a full record of events. The Head of Quality and Curriculum who manages the quality management system is responsible for working with the Head of Operations in recording the incident within the critical incident log.

The log will review trends in incidents, timeframes for resolution, and impact to ensure further preventative actions are implemented where possible.