Business Continuity Plan
Coping with a Serious Unexpected Incident

A practical guide for businesses to use and develop an incident response/business continuity plan.

Introduction

Business Continuity Management (BCM) is no longer an optional activity. Too many people still do not understand what BCM is really about. They regard it as an operational response to large-scale incidents, usually involving significant asset loss.

BCM is about finding strategic solutions to the loss of one or more of seven significant resources:

- Staff;
- Facilities;
- Technology;
- Customers or service users;
- Key Suppliers;
- Cash-flow; and,
- Goodwill.

Being properly prepared to deal with unexpected interruption to any of these resources is at the heart of any business continuity strategy. BCM is the only real methodology that delivers such resilience across the entire range of business activity. This may be considered commercial 'best practice' as, by planning now rather than waiting for an event to happen, your business can get back to normal in the shortest possible time.

A key part of BCM is the Business Continuity Plan (BCP). Where disruption affects critical business activities the consequences can be severe and may include substantial financial loss, an inability to achieve desired levels of service, embarrassment and/or loss of credibility within the community. The benefit of having a business continuity/recovery plan that can be implemented with the minimum of fuss and delays, significantly reduces the levels of disruption your business suffers and ensures rapid resumption of 'normal service' to your customers.

A business continuity plan should cover a range of potential significant incidents that could occur, for example incidents that result in the business needing to evacuate its premises whilst open to the public and the building(s) not being immediately available for reoccupation, such as:

- Fire, flood or explosion;
- Chemical or toxic substance release;
- The effects of disasters in the wider community.

There may also be specific hazards or events that pose a particular risk to your business, such as proximity to an industrial site, river or major road, or cause significant disruption to your business operations (e.g. serious injury or death on site).

The plan should make an assessment of any specific risks affecting your business and explain in detail how an incident arising from the hazards will be dealt with.

The Planning Process

It is important to involve your staff in the planning process to ensure that they support the plan and are able to implement it in the event of an incident.

Businesses should identify staff who are prepared to take on roles during an incident. One member of staff should take responsibility for updating and reviewing the plan once it is in place.

Preparing the Business Continuity Plan (BCP)

If an incident occurs and the business is closed for any reason (e.g. severe weather) it is likely that staff or customers may try to telephone your business to get information. This may hamper those of your staff dealing with the incident itself. One possible way of dealing with this is to set up on your main telephone line an answer machine that you can set to “message only” (callers cannot leave messages, but can listen to an update on the position). Updating the message regularly with information on the emergency will ensure that staff and customers are informed of the current position, without tying up valuable staffing resource.

If updates to the message are not possible (due to evacuation of premises for example), the message should point the listener to where updated information can be obtained, such as a local radio station(s) or any helpline set up by the authorities, or even your own website, should you have one.

Other methods of informing staff and customers that you may be able to use are:

- Notices on your website, should you have one;
- E-mails or text messaging;
- Telephone;
- Notices on the entrances to your premises;
- Person at the entrance to your premises to verbally explain issues;
- BBC local radio – if a significant incident, the BBC have a duty to ‘warn and inform’ the public.

In order to carry out the procedures outlined in your plan some awareness raising and training must be undertaken with your staff. All staff have a role in the plan and should be aware of the full scope of the plan and their place within it. Staff that may not be specifically identified as a part of the response to an incident should, nevertheless, be aware of the content of the plan - particularly the sections on emergency contact, evacuation and shelter.

The Business Continuity Plan (BCP)

The following paragraphs give some ideas which you may wish to include within your plan or think about the implications for your business. Many of these will depend on the size and complexity of your business and premises. A pro-forma plan that you may wish to use is attached as Appendix A.

The plan should be kept short and simple but include information which may be required when the plan is activated.

The plan should identify who is authorised to activate it and how this will be done (usually the Managing Director/CEO/Senior Manager/Duty Manager will do this and there will be a communication procedure to be followed).

If an incident occurs during normal business hours, the first priority should be to safeguard customers and staff and to alert the emergency services, if necessary. After this, if this is a major incident, the Local Authority Emergency Management Team may need to be informed.

The incident management team leader, a pre-assigned nominee, will take overall responsibility for the business’s response to the incident. This person should be supported by an incident management team. Lead staff (and deputies) to be identified along with designated helpers for each group or separate work areas you may have.

A place of safety must be identified for when the building needs to be evacuated. Should customers and staff need to be away from your premises for a sustained period of time, shelter must be a consideration. A “buddy” arrangement with another local business or a community centre, leisure centre or a church hall, might meet this need. If a local park, car park or other outdoor venue is used then arrangements to protect customers and staff from adverse weather needs to be a consideration.

It is vital to construct a list of contacts that will be of use in the event of an incident. This must not only include key support agency/organisation contact details but also emergency contact details for all your staff and your key business contacts and suppliers. This data should be kept in an emergency pack or 'grab bag' as appropriate. The plan should identify the location of any emergency pack or 'grab boxes' and ensure your staff know where these are located and what they contain.
See Appendix 4 for more details on grab bag.

Can the business be split into sections (if the business is large enough to have multiple buildings on site; employ many teams of staff within different parts of one building etc.)? This may make managing an incident easier. Consideration must be given to the size of the business and its premises and the easiest way of managing the numbers of staff or customers likely to be involved.

An emergency communications contact should be identified. This person will deal with urgent communications with the emergency services, the local authority, the press/media etc. If possible, this person would not be communicating with customers and staff, but may well compile the message to be given to customers and staff, thus ensuring consistency of message.

Security arrangements should be made that will ensure, so far as reasonably practicable that the business premises/site will be secure whilst it has been evacuated.

Welfare arrangements for both customers and staff should be considered, for example are there toilet facilities, drinking water and feeding arrangements in any premises used to house evacuated staff and customers. First aid arrangements must be clear. First aiders should be identified and trained. The establishment of visible first aid points at the evacuation site may be an idea to consider.

The action cards at Appendices 6a and 6b provide a checklist to use during an incident. It is important that all staff are aware of these checklists and they are readily available – they could be placed close to your usual or emergency exits to be grabbed on the way out.

It may be worth including a plan of the premises (for use by emergency services) showing locations of:

- Main water stop-cock
- Switches for gas and electricity supply
- Items that would have priority if salvage becomes a possibility
- Any hazardous substances stored on site

Appendix A: Pro-Forma Business Continuity Plan Template

Business Continuity Plan

NAME OF BUSINESS

Address of business

Telephone number of business

E-mail address of business

UPDATED	
AUTHOR	
DOCUMENT OWNER	
VERSION No	
NEXT REVIEW	

CONTENTS

How to use this plan

1.1 The Business Continuity Standard states –

"In any incident situation there should be a simple and quickly-formed structure that will enable the business to:

- Confirm the nature and extent of the incident
- Take control of the situation,
- Contain the incident, and
- Communicate with stakeholders"

This template is not intended to be a prescriptive list of actions to manage any incident but forms a basic structure upon which an effective response can be built. If the incident does not require a full Business Continuity response but has a significant impact on service delivery, please refer to the Sudden Unexpected Incident Guide at Appendix 1.

This plan also aims to identify alternative accommodation the business will require in the event of both a short or long-term loss of facility.

Business continuity arrangements should be tested regularly and any lessons learned incorporated into the BCP as soon as possible.

This template draws together the resources, data and procedures which the business needs to enable it to run in a crisis. When completed it should contain:

- Key people and their contact numbers (staff, key suppliers, service users/customers. See section 8 for contact details
- Alternative locations (current, recovery site, area for staff to go where they await site availability)
- ICT/procedures for running service, equipment, technology, records etc. needed
- Any external/third party disaster recovery agreements the business may have
- Actions necessary in first 24/48hrs, and the next week
- Sample log for decisions and actions (see Appendix 2)

Plans should reflect the recovery phases, keeping them as brief as possible. Ensure it is understandable and useable by staff who may be called upon to respond during an incident.

Phase 1	First 24/48 hours	Essential urgent tasks. Temporary arrangements to provide the most essential parts of service. Critical staff only required on site.
Phase 2	Days 2-7 (first week)	Start restoring the most essential parts of service. Ensure temporary working practices introduced in first 24 hours are robust and fit for purpose.
Phase 3	Following week	Plan and begin restoring remaining parts of the service.
Phase 4	Until 'business as usual'	Restoring full service and return to normal working. Hold a de-brief to learn from management of the incident.

1.2 Briefing of Staff Training & Exercising

It is important that staff are fully briefed on its contents and given the opportunity to train and exercise its key elements. All such briefing, training and exercising should be recorded using a table similar to the one shown below. The business continuity arrangements should be tested from time to time to ensure that staff understand their roles and responsibilities during an incident.

Records of BCP Tests/ Emergency Management Exercises

Date	Description of Briefing Test Exercise	Parties Involved in Test

Incident Management Team

2.1 Incident Management Team structure

The Incident Management Team is made up of the Senior Management Team of the Business. The team informs and reacts at the time of/as soon as possible after the incident. On forming, those present should take decisions to apply appropriate resources to deal with any events as they occur (ideally to prevent the incident becoming a crisis).

The key roles of the Incident Management Team are to:

- Provide strategic direction, especially at a local level
- Activating and standing down the Business Continuity Plan
- Safeguarding the welfare of staff, contractors and visitors
- Represent the public face of the business
- Liaise and communicate with stakeholders, e.g. staff, customers, suppliers and, if applicable, the Local Authority
- Assume responsibility for co-ordinating incident management and prioritising the recovery of key activities
- Provide direction/support as required to staff and outside agencies to effectively manage the incident at an operational level
- Test the business continuity arrangements from time to time

All decisions, actions and other relevant information should be logged using a Decision / Action log sheet (a possible format can be found at Appendix 2). It is advisable to appoint a 'scribe' or 'loggist' at the start of the incident. This is best left to someone who is not going to have (significant) recovery tasks allocated to them. It may also be worthwhile logging decisions and actions that were deemed unsuitable or were not taken and include the rationale behind them. If required, commence a financial expenditure log to record financial expenditure incurred during the course of the incident (See Appendix 3 for a possible format of a Financial Expenditure Log template).

2.2 The Incident Management Team

The table below should show the members of the Incident Management Team

Name	Role	Contact details
	Managing Director	
	Senior/ Deputy Manager	
	Duty Manager	

2.3 Incident Management Team Meeting Rooms

Establish an Incident Management Team Meeting Room so that dealing with the event can be coordinated from one place rather than have members of the Incident Management Team dispersed

This table should show which rooms would be used by the Incident Management Team from which they may manage the response to an incident.

	First Choice	Second Choice (offsite option)
Nominated Meeting Rooms		
Capacity		
Computer Equipment Held in Room (PCs, lap tops, printers etc)		
ICT Network Points in Room		
Telephone Points in Room		
Other Specialist Equipment Held if Necessary (e.g. Digital TV & Radio, fax)		
Status of Meeting Room (Red – Room unlikely to be fully operational within up to half a day; Amber – room will take around one to two hours to be ready; or Green – room ready at all times.)		
Toilet Facilities available (Y/N)		
Separate Room Available (for meeting staff, press etc)		
Emergency Pack Available (see Appendix 4 for suggestions)		

Incident escalation and Invocation procedures

Incident escalation and invocation of the Business Continuity Plan

3.1 Incident Escalation Process

It is vital that the business has a clear and simple method by which it can quickly recognise a business continuity threat and act accordingly. It is generally better to over-react to serious incidents and then stand down staff than to under-react.

The agreed escalation and invocation framework to be adopted and understood by all is set out below.

- Incident reported to Managing Director/CEO/Senior Manager/Duty Manager
- They take the decision as to whether the Business Continuity Plan needs to be invoked
- Advise Head/Regional/Area Office (if appropriate)

The Managing Director/CEO/Senior Manager/Duty Manager has the authority to compel all other managers and staff (as relevant) to meet as soon as is reasonable as the Incident Management Team to discuss an incident, or the threat of an incident, which could mean the Business Continuity Plan being invoked.

These will be incidents of concern that will trigger the Corporate Plan in whole or in part. **THESE ARE CORPORATE BUSINESS CONTINUITY EVENTS.** The triggers include:

- Threat to life or wellbeing of significant numbers of staff, customers, contractors, visitors;
- Death or serious injury to staff or those in the care of the business;
- Loss of strategic leadership;
- Insufficient staff to keep a Business Critical Activity running;
- Key individuals unavailable (single critical knowledge source);
- Any Business Critical Activity is inaccessible or degraded to the point where service provision is becoming impossible;
- Loss of key assets (e.g. premises, vehicles);
- Significant ICT failure (central ICT, telecoms, critical business systems);
- Failure of a key supplier or other third party on whom the business is heavily reliant;
- Potential for significant financial loss (causing unplanned cuts or fundamental change in revenue strategy, or loss of stakeholder confidence);
- Local, regional or national emergency which impacts on the business's ability to deliver essential services;
- Major disruption to essential functions, caused by any means including flood, fuel crisis, pandemic or terrorist attack.

The Incident Management Team will continue to direct the continuity and recovery operations. There may be elements of the response that become business continuity and recovery at differing times or can be both business continuity, recovery and incident response e.g. the Communications Team may be required to continue to issue updates on the management of the incident and, at the same time, begin to alert staff and customers to changes in business delivery that will be necessary in the days or weeks ahead. It is important that there are regular, continuing employee/customer communications and safety briefings all the way through to 'business as usual' being restored.

The Incident Management Team Lead should ensure that recovery staff are briefed to deal with any damage that may have occurred to premises and check that the recovery is proceeding as expected at regular intervals - taking any necessary action to resolve any unforeseen problems that may be delaying the recovery. Until 'business as usual' resumes, the recovery staff should continue to report to the Incident Management Lead.

Carry out debrief of the incident and document opportunities for improvement and any lessons identified. Review the BCP in light of the lessons learnt from the incident and the response to it.

Phase 1

4. Incident Management Phase (First 24 hours)

Purpose:

- Protect the safety and welfare of staff, visitors and the public
- Protect vital assets e.g. equipment, data, reputation
- Ensure urgent and necessary communication takes place
- Support the Business Continuity phase
- Support the Recovery and Resumption phase

	REQUIREMENT	ACTION	ACTION DONE?	BY WHO?
1.	Make a *quick* initial assessment: ▪ Survey the scene/situation ▪ Assess the impact on staff other stakeholders ▪ Assess scale/severity, duration & impact ▪ Disseminate information (to others) ▪ Call the Emergency Services if needed ▪ Evacuate the premises if necessary	Gather and share information to facilitate decision-making and enhance the response. See Appendix 5 for an Incident Impact Assessment form	☐	
2.	Ensure a log of key decisions and actions is started and maintained throughout the incident	See Appendix 2 for template of Decision/Action log	☐	
3.	Where appropriate, record names and details of any staff / visitors / contractors etc that may have been injured or affected by the incident as part of your incident record keeping.	This information should be held securely as it may be required by Emergency Services or other agencies during or following the incident.	☐	
4.	Log details of all items lost by staff, visitors etc as a result of the incident, if appropriate	See Appendix 2 for template of Decision/Action log	☐	
5.	Assess the key priorities for the remainder of the working day and take relevant action	Consider actions to ensure the health, safety and well-being of staff, visitors, contractors at all times. Consider your business continuity strategies, i.e. alternative ways of working, re-location to your recovery site etc to ensure the impact of the disruption is minimised. Business Continuity Strategies are documented in Section 5	☐	
6.	Log all expenditure incurred as a result of the incident	Record all costs incurred as a result of responding to the incident. See Appendix 3 for a Financial Expenditure log.	☐	
7.	Consider your communications strategy to ensure staff and relevant stakeholders are kept informed about what is required of them. If the incident is taking place outside of normal working hours, staff may need to be contacted to advise of any alterations to normal working arrangements for the next day.	All staff member's emergency contact details should be held securely electronically as well as in a hard copy as part of your plan. .	☐	

Phase 2

5. Business Continuity Phase

Purpose

- To ensure that 'critical activities' are resumed as quickly as possible and/or continue to be delivered during the disruption
- To activate one or more of your business continuity strategies to enable alternative ways of working
- To make best use of potentially limited resources by suspending 'non critical' activities

Time Critical Activities

The purpose of the business continuity phase of your response is to ensure that critical functions are resumed as quickly as possible and/or continue to be delivered during any disruption. This may involve activating one or more of your business continuity strategies to enable alternative ways of working. During an incident it is unlikely that you will have all of your resources available to you, it is therefore likely that some 'non critical' functions may need to be suspended at this time.

Table 1, below, is a list of many critical activities carried out by the business and the maximum time it could run without performing them. Feel free to add to these as appropriate.

Table 1 – Critical Activities

Function Details					Resource Requirements				
	Critical Function	**MTPD**	**RTO**	**Minimum Service Level**	**Staff**	**Data/ Systems**	**Premises**	**Equipment**	**3rd Party Dependencies**
1	*Payroll*								
2	*Catering*								
3									
4									
5									

MTPD – Maximum Tolerable Period of Disruption

RTO – Recovery Time Objective

Table 2 – Requirements to re-Instate Full Service

Requirement	Considerations
Building	Secure, appropriate and fully risk-assessed with all utilities connected and working. Full working catering facilities.
Transport to and from temporary accommodation	For staff, if necessary at an appropriate, safe place.
Toilet facilities	Suitable for the number and gender of staff and customers
Office facilities	Appropriate for the number of staff and with appropriate furniture
Staff area	With tea / coffee making facilities etc.
Telephones	With at least two lines
Computers	Ideally at least one per office / shop floor area. Also for administrative use.
Internet access	Ideally in each of the office facilities
Printers	Ideally enough to support your administrative needs
Photocopiers	Black and white sufficient
Stationery	Appropriate and sufficient exercise books, paper, pens, pencils, rulers, erasers etc.

NB - These requirements will not be all of those that you may have. Some may not be applicable to the business and you may want to add others. These are here as a guide only.

	REQUIREMENT	ACTION	ACTION DONE? *(Check box accordingly)*	BY WHO? *(Insert details of responsible Officer)*
1.	Take time to understand and evaluate the impact of the incident on 'business as usual' activities by communicating with key stakeholders to gather information.	Depending on the incident, you may need additional/specific input in order to drive the recovery of critical activities. This may require the involvement of external partners.	☐	
2.	Plan how critical activities will be maintained, utilising pre-identified or new business continuity strategies	Consider: ▪ Immediate and ongoing priorities ▪ Communication strategies ▪ Resource availability ▪ Deployment of resources ▪ Roles and responsibilities ▪ Finance ▪ Monitoring the situation ▪ Reporting ▪ Stakeholder engagement ▪ Any welfare issues ▪ Planning the recovery of non critical activities	☐	
3.	Identify any other stakeholders who may be required in the business continuity response	Depending on the incident, you may need additional/specific input in order to drive the recovery of critical activities; this may require the involvement of external partners.	☐	
4.	Log all decisions and actions, including what you decide not to do and include your decision making rationale.	See Appendix 2 for template of Decision/Action log	☐	
5.	Log all financial expenditure incurred as a result of the incident	Use the Financial Expenditure log which can be found at Appendix 3	☐	
6.	Deliver appropriate communication actions as required	Ensure methods of communication and messages are developed as appropriate to the needs of your key stakeholders e.g. Staff, Partners, Suppliers etc.	☐	

The main impacts of interruptions on organisations fall broadly into the following categories – **The Four Ps'**. Planning for these will enable you to deal with most incidents. This should consider the following factors:

Loss of <u>People</u>	Could be – high staff absence, total staff loss (e.g.on strike), key individual(s) unavailable
Loss of <u>Premises</u> **Or other key assets e.g. vehicles**	Could be – loss of facilities (e.g. power cut), temporarily unable to access building (e.g. floor or police incident), or destruction of building (e.g. total loss through fire or explosion
Loss of <u>Plant</u>	Could be – loss of ICT systems, loss of network, loss of hard/software , loss of telephones/Lync system
Loss of Key Supplier/<u>Partner</u>	Could be – temporary (e.g. dispute, disruption to supplier's business) or permanent (e.g. supplier goes out of business or cancels contract)

Loss or unavailability of staff

Think about what staff you will need to cover the loss. How many? What skill sets? What qualifications? What security clearances? Which agency will you use? The table on below lists actions that may need to be taken if staff were unavailable. It is not an exhaustive list of actions. Please feel free to amend/add actions according to what is relevant for the business.

Loss or unavailability of premises

Think what you will do immediately, what arrangements you can make to access locations you need and get the equipment etc that is necessary for the business. You may want to consider reciprocal arrangements with customers and suppliers. Include here the actions to let staff, customers, suppliers, local community know where you are moving to and how they may contact you. The table below lists actions that may need to be taken if the premise was unavailable. It is not an exhaustive list of actions. Please feel free to amend/add actions according to what is relevant for the business.

ICT failure (system, network, telecoms)

Think what you will do if you have ICT failure e.g. consider work on standalone PCs/laptop or manual working. Consider how many staff have access to mobiles/blackberry devices etc. Find out (if you have an external service provider) whether any of the applications are web based. Also, does software have to be installed on to a device to operate a web based solution? *The table below lists actions that may need to be taken if ICT System was unavailable. It is not an exhaustive list of actions. Please feel free to amend/add actions according to what is relevant for the business.*

Loss of Key Supplier or Service Partner

Are you reliant on a supplier providing you with a key service or product? Have you considered the impact to the business of losing a critical supplier and how long it would take to find an alternative source? Do you know the current financial status of your supplier? Your supplier may be planning cutbacks that may affect you. The table below lists actions that may need to be taken if suppliers were unavailable. It is not an exhaustive list of actions. Please feel free to amend/add actions according to what is relevant for the business.

TACTICAL OPTIONS TO MITIGATE AGAINST LOSS OF STAFF OR SKILLS		ADDITIONAL INFORMATION
1.	Use of temporary staff	
2.	Multi-skilling/cross training to ensure staff can undertake different roles and responsibilities. This could involve identifying deputies /job shadowing/staff undertaking temporary additional duties	
3.	Using different ways of working to allow for a reduced workforce	
4.	Suspending 'non-critical' activities to focus on your priorities	
5.	Ensuring that the business continuity aspects of staff management are considered in all management arrangements, e.g. managing attendance, job descriptions, contractual requirements etc.	
OPTIONS TO MITIGATE AGAINST LOSS OF PREMISES		**ADDITIONAL INFORMATION**
1.	Identification of alternative locations designated as the agreed recovery site. You will need to consider transport requirements and accessibility for these identified premises. You may need to have multiple places agreed for your recovery site if you have large premises and these different options will need to be documented.	
2.	Creating an emergency 'grab bag' (see Appendix 3 for suggestions) that contains essential information and equipment needed for both incident management and business continuity, and should be stored in a secure place on and off site. The contents of the bag should be the responsibility of a named person and should be regularly checked and updated	
3	Are they any reciprocal / mutual arrangement with other organisations where there is capacity to accommodate each other in the event of an incident?	
4	Localising the incident, e.g. isolating the problem and utilising different sites or areas within the premises portfolio	
OPTIONS TO MITIGATE AGAINST LOSS OF PLANT (ICT SYSTEMS INCLUDING TELEPHONY)		**ADDITIONAL INFORMATION**
1.	Use of a secure external network, virtualised network or secure cloud that can be accessed via the internet to allow extra back up and protection for your files	
2.	Manual workarounds: ensure there is a record of where pre-printed forms etc are stored and that there are procedure guides to inform their use where necessary	
3.	Access systems via the internet outside of your network for secure, cloud based applications.	
4.	Ensure that anyone who requires ICT to undertake critical activities has the ability to work at home where possible and appropriate. Ensure that critical equipment is taken home where practical and possible and consider procuring mobile equipment for these users.	
5.	Using different ways of working. This could include: changing work patterns, suspending 'non critical' activities to focus on your priorities and assist the recovery of critical systems in the first instance with a phased approach for all other ICT 'non critical' activities.	

TACTICAL OPTIONS TO MITIGATE AGAINST LOSS OF A KEY SUPPLIER, THIRD PARTY OR PARTNER AGENCY		ADDITIONAL INFORMATION
1.	Pre-identified alternative suppliers	
2.	Ensuring all external providers have a Business Continuity Plan in place and you understand the impact to their plan on the delivery of your critical activities in the event of an incident	
3.	Insurance cover	
4.	Using mutual support agreements with other businesses, if possible	
5.	Using alternative ways of working to mitigate the loss, e.g. suspending activities.	

Phase 3

6. Recovery and Resumption

Purpose

- To return to 'business as usual' as quickly as possible
- To ensure any non critical activities suspended as part of the business continuity response are recovered within appropriate timescales
- Where the impact of the incident is prolonged, normal operations may need to be delivered under new circumstances e.g. from a different building on a longer term basis.

	REQUIREMENT	ACTION	ACTION DONE? *(Check box accordingly)*	BY WHO? *(Insert details of responsible Officer)*
1.	Agree and plan the actions required to enable recovery and resumption of normal working practises	Agreed actions will be detailed in an action plan and set against timescales with responsibility for completion clearly indicated.	☐	
2.	Continue to record all expenditure incurred as a result of the incident	Use the Financial Expenditure Log (Appendix 5) to record any expenditure	☐	
3.	Respond to any ongoing and long term support needs of staff.	Depending on the nature of the incident, the Incident Management Team may need to consider the use of health services, for example counselling.	☐	
4.	Once recovery and resumption actions are complete, communicate the return to 'business as usual'.	Ensure all staff are aware that the Business Continuity Plan is no longer in effect.	☐	
5.	Carry out a 'debrief' of the incident with Staff and Suppliers/Partners if appropriate. Complete a post incident report to document opportunities for improvement and any lessons identified.	The incident de-brief report should be reviewed by all members of the Incident Management Team to ensure that key actions resulting from the incident are implemented within designated timescales.	☐	
6.	Review this Business Continuity Plan in light of lessons learned from the incident and the consequent response to it	Implement recommendations for improvement and update this Plan.	☐	

Emergency Management Guidance

7. Other Emergency Incidents / Considerations

Serious emergencies affecting a business like a serious fire, physical assault, threat of mass harm to staff, are thankfully very rare. However, they do occur and it is important that the business is ready to respond to such events in a coordinated, pre-planned, effective fashion to minimise the impact wherever possible.

All businesses must have robust and regularly rehearsed fire evacuation procedures with well-maintained fire-fighting equipment, fire / smoke detection and alerting systems, clearly signed evacuation routes / exits and appropriate evacuation assembly areas. However, it is important to pre-plan for the other types of emergency too.

Serious Physical Threat Person or Explosive Device
In such circumstances the priority is to keep as many staff as possible isolated from the actual or potential perpetrator or threat. Each incident is likely to be different but it is good practice to consider what parts of the business and its grounds can be physically secured from other parts and also how this could be achieved swiftly should the need arise.

It is also important that where a dangerous person is at large or a suspect item identified it is understood that normal fire evacuation procedures will not be appropriate and the **FIRE ALARM SHOULD NOT BE ACTIVATED**. Indeed, it may be safer for staff to stay where they are and secure that part of the building or even to "invacuate" (the movement of people to safe and secure locations within buildings rather than leaving the buildings in a conventional evacuation). A site plan of the business showing potentially securable zones will aid planning in this regard. Because each incident is likely to be different and therefore the response tailored to the specific circumstances, a series of action cards might be developed to assist an effective decision making process. Examples of such action cards can be found at **Appendices 6a - 14**. These could be laminated and available for quick reference at key locations within the business.

Whatever the circumstances of an incident, effective communication between staff within different parts of the premises is vital and pre-planning as to how this can best be achieved should form a central part of the emergency plan.

8. Contact Details

Key Contacts			
Name and Role	**Mobile No.**	**Work No.**	**Home No.**

External Partners & Suppliers		
Contact Type	**Additional Information (e.g. contact names and/or account numbers)**	**Contact Numbers**

External Partners & Suppliers		

Appendix 1

Sudden Unexpected Incidents Guide

Has there been a death or serious injury to anyone?

Yes	No
First 30 minutes	
Call appropriate Emergency Services - if not already in attendance; Make sure area is secured; Report to Security Team; Inform Health and Safety Team; Inform Head of Service to act as Lead; Commence/keep a log of events/telephone calls and key decisions; Advise staff involved not to make any statements to Police/HSE until Legal advice has been given; Lead Head of Service to inform your Strategic and Divisional Directors; Inform Human Resources to enable access to Next of Kin information (if staff member). Inform Communications team	Inform Head of Service to act as Lead; Commence/keep a log of events/telephone calls and key decisions; Lead Head of Service to inform Strategic and Divisional Directors; If property damage, inform Property Services; If incident relates to ICT, inform Head of ICT: Inform Communications team Consider if Health and Safety need to be informed and/or an SO2 done
First 2 hours	
Convene meeting of Senior Management Team if necessary; Consider whether there is a need to invoke your Service BCP; Issue Press statement – Incident Lead/Comms Team (Press Desk); Consider statements via social media – Comms Team; Inform immediate team of event; Advise all staff present to say nothing to press/media and pass all queries to Press Desk; Advise Unions – if appropriate;	Convene meeting of Incident Management Team if necessary; Consider whether there is a need to invoke your Service BCP; Issue Press statement – Incident Lead/Comms Team (Press Desk); Consider statements via social media –Comms Team Inform immediate team of event; .
First 24 hours	
Update Press statement – Incident Lead/Comms Team (Press Desk); Witnesses/Colleagues – Provide counselling contact details (AMICA); Consider flowers/letter of sympathy (if serious injury or fatality); Health and Safety Team to commence collation of documentation.	Update Press statement – Incident Lead/Comms Team (Press Desk).
Following Week(s)	
Update Strategic Directors/Heads/Staff/Press; Inform Human Resources – (regards salaries/stop correspondence to deceased in cases of fatality); Attendance at funeral/inquest – if fatality; ICT – Removal of photos from websites/Outlook – if fatality or return to work unlikely; Sympathetic removal and return of personal belongings – if fatality or return to work unlikely.	Update Strategic Director/Heads/Staff/Press

Sudden Unexpected Incidents Guide

This guide will relate to significant unexpected incidents within the service such as fatal or serious injuries, major property damage, major financial loss or breaches of the Law. This does not supersede any Tactical procedures you may have within your service, but is intended to complement them. This should be used in conjunction with, and not instead of, your Business Continuity Plans, if appropriate. The list has been compiled to cover other eventualities; hence some of the actions will only be needed if the Lead Officer deems them to be appropriate.

Useful Contact Numbers

Chief Executive – **NAME – Work – Mobile – (TO BE COMPLETED BY AREA BEFORE ISSUE TO MANAGERS)**

Strategic Director – **NAME – Work – Mobile – (TO BE COMPLETED BY AREA BEFORE ISSUE TO MANAGERS)**

Divisional Director – **NAME – Work - Mobile – (TO BE COMPLETED BY AREA BEFORE ISSUE TO MANAGERS)**

Head of Service – **NAME – Work – Mobile – (TO BE COMPLETED BY AREA BEFORE ISSUE TO MANAGERS)**

Insurance Team – **NAME – Work – Mobile – (TO BE COMPLETED BY AREA BEFORE ISSUE TO MANAGERS**)

Health and Safety Team – **NAME – Work – Mobile – (TO BE COMPLETED BY AREA BEFORE ISSUE TO MANAGERS)**

Risk Management – **NAME – Work – Mobile – (TO BE COMPLETED BY AREA BEFORE ISSUE TO MANAGERS)**

Business Continuity Guidance/Support – **NAME – Work – Mobile – (TO BE COMPLETED BY AREA BEFORE ISSUE TO MANAGERS**)

Emergency Management – **NAME – Work – Mobile – (TO BE COMPLETED BY AREA BEFORE ISSUE TO MANAGERS**)

Communications Team – Press Desk – **NAME – Work – Mobile – (TO BE COMPLETED BY AREA BEFORE ISSUE TO MANAGERS)**

Customer Services – **NAME – Work**

Human Resources – **NAME – Work**

Payroll – **NAME – Work**

Property Services – **NAME – Work**

BRO/Premises Officer/Facilities Management - **NAME – Work – Mobile**

Appendix 2

LOG OF DECISIONS, ACTIONS, CONTACT and OTHER EVENTS

A log of events is to be maintained by the business

Incident _____		**Date**
Time	Record Assessment / Decision / Action / Outcome	Loggist Initials

Appendix 3

FINANCIAL EXPENDITURE LOG				
Completed By		**Incident**		
Date		**Time**		
	Expenditure Details *(what, for whom etc)*	**Cost**	**Payment Method**	**Transaction made by**

Appendix 4

Guidance for Content of an Emergency Pack/Grab Box

One of the most useful actions that you can take to cope with an incident is to have an 'Emergency Pack/Grab Box' prepared in advance. This is a pack of items that will help you implement your plans. Ensure packs are stored safely and securely off site (in another location and items in the pack should be checked regularly, be kept up to date and be working). Person(s) responsible for the grab box is//are mentioned in this plan. You may need to lock it away due to the sensitive nature of the content of the box but ensure not only one person has access to where it is locked. Remember that cash or credit cards may be needed for emergency expenditure in the early stages of response to an incident. Dependent upon your service area, items that you may wish to include are:

Documents

- Business Continuity Plan – hard copy of your plan to recover the business or service;
- List of employees with contact details – include home and mobile numbers and even e-mail addresses. You may also wish to include next-of-kin contact details.
- List of key customer/supplier details.
- Contact details for emergency glaziers, salvage organisations and building contractors.
- Contact details for utility companies.
- Building site plan (this would be helpful in a salvage effort), including location of gas, electric and water shut off points.
- Latest inventory list.

Equipment

- Computer back up tapes/disks/USB memory sticks or flash drives.
- Spare keys and security codes.
- Torch and spare batteries.
- Hazard and cordon tape.
- First Aid kit.
- Message pads and flip chart.
- Marker Pens (for Emergency Signage).
- General; stationery (pens, paper etc).
- Mobile telephone with credit available, plus charger.
- Dust and toxic fume masks.
- Disposable camera (for recording evidence for any insurance claim).
- Whistles and High Visibility jackets.

Ensure you are able to repair or replace any equipment vital to your service delivery at short notice. If you are able to, consider storing spare parts off-site.

This list is not exhaustive and there may be other documents or equipment that should be included for your area.

Appendix 5

INCIDENT IMPACT ASSESSMENT FORM	
Completed By	
Date	
Time	

Consideration	**Logged Response**
Which department is affected	
What is the nature of the incident? (Describe the type of incident, location and severity)	
Are there any staff casualties or fatalities? (Complete casualty / fatality sheets if needed)	
How is the incident currently affecting business operations?	
What is the estimated duration of the incident?	
Do the Emergency Services need to be called?	
Has access to the whole site been denied? If so, for how long?	

Have any work areas been destroyed, damaged or made unusable? Is there evidence of structural damage?	
Are any systems and other resources unavailable? (include computer systems, telecoms and any other assets)	
Have any utilities been affected? (E.g. gas, electricity or water)	
Other relevant information	

Appendix 6a

Action Card - Evacuation

1. Call Emergency Services (police/fire/ambulance) if necessary. Will help to have the following information available if possible:

   - **C**asualties - Approximate numbers of dead, injured and uninjured
   - **H**azards - Present and potential
   - **A**ccess - Best access routes for emergency vehicles, bottlenecks to avoid etc.
   - **L**ocation - The precise location of the incident
   - **E**mergency - Emergency services already on scene, and what others are required
   - **T**ype - Type of Incident, including details of numbers of vehicles, buildings etc. involved
   - **S**tart a log

2. Pick up emergency pack(s)/grab box(es)
3. Collect essential medicines (ensure these remain tightly controlled) if possible
4. At evacuation point take register

Appendix 6b

Action Card – Invacuation

1. Ensure all staff, visitors and contractors are inside the building or part of a building
2. Close and lock all outside doors and windows
3. Contact the police on 999 if life is in danger or there is a risk of significant harm
4. Shut off any air conditioning units which link to outside
5. Registers should be taken to ensure all present
6. If a dangerous person is at large, try and stay away from the part of the building / site which they can access. Stay away from windows, consider barricading doors, hide behind as substantial cover as possible, stay quiet, and turn off mobile phones to avoid detection by them. Wait for the police to respond unless a clear opportunity to escape safely with your staff presents itself.

Appendix 7

Suspected Explosive / Incendiary Device

If you discover a suspected explosive or incendiary device, please refer to the following:

- If anyone is touching the suspected device, **PUT DOWN IMMEDIATELY.**
- Otherwise **DO NOT** touch it at all.
- Inform the most senior member of staff available and the police on 999 if not already in attendance.
- If possible, open all doors and windows and evacuate all staff, asking them to take all personal belongings.
- If possible and practical, leave a marker near the device and show an improvised route to the most suitable entry point.

- **DO NOT** lock doors.
- **DO NOT** operate any lights.
- **DO NOT** use mobile phones or radios within 15 metres.
- **DO NOT** re-enter the area.
- **DO NOT** place the device in water/sand.
- **DO NOT** cover the device.

- Should this be reported, it is the responsibility of the most senior member of staff available on site to take charge as the incident coordinator.
- If you suspect a hoax, remember that it is a still a criminal offence and information should still be recorded as well as evidence preserved.
- If a search is decided upon, staff members who are familiar with the area should conduct this, as they are most likely to identify something alien.

- **Minimum cordon distances:**
  - Up to briefcase size: 100 metres
  - Up to small vehicle size: 200 metres
  - Large vehicle size: 400 metres

- If a letter or very small package a more limited evacuation is appropriate consisting of the room containing it, adjacent rooms (two in each direction from the device room). The same being applied to rooms two floors above and below the device
- It is important to remember that evacuation can become dangerous in the event that the location if the device is unknown. The assembly points will not normally be the same as the fire evacuation assembly points so the fire alarm **MUST NOT** be sounded.
- Considerations for suitable pre identified routes should include the potential for secondary devices.
- When an incident occurs, the nominated assembly point should be checked for secondary devices as soon as possible.
- It is also good practice to pre determine suitable protected spaces within your building as if the suspected device is next to the exit or in the street it is usually better to shelter inside the building away from windows and behind protective structural walls

Appendix 8

Suspected Contaminated Mail

If you discover a suspicious item inside a building and you suspect chemical, biological or radiological material, please refer to the following:

- If the item is still intact, **DO NOT** shake, squeeze or open it. If you are already holding the item, place in a transparent, sealable plastic bag or container, or cover with anything to hand (e.g. clothing, paper, waste bin, etc). **DO NOT** remove this cover.
- **DO NOT** touch, tamper with or move the item.
- **Turn off** all air conditioning, fans, photocopiers, printers, computers and heaters.
- Close all windows and doors and evacuate the room. Leave the keys in the lock.
- If possible and practical, place a clear, visible warning on the door.
- If any content spills onto an item of clothing, remove that clothing immediately. **Do not** rub your eyes, touch your face or any other person. Wash your hands with soap and water as soon as possible.
- Go to an isolated room and avoid contact with any other person, if possible. Ensure to segregate yourself and others who have come into contact with the package.
- Reassure your colleagues, it is unlikely that they have become contaminated, but they will receive medical treatment if required.
- Ensure you have access to a phone. The emergency services are likely to want to contact you directly.
- If possible, have someone who has not been in contact with the suspect item to meet with the emergency services.
- Do not be alarmed if the emergency services arrive wearing protective clothing, this is common practice.
- Inform the police on **999** and the most senior member of staff available**.**

If a suspect item is outside a building:

- Move away from the item, against the wind, as far as possible. Allow the police to confirm whether the item is suspect or not.

Appendix 9

Suspicious Behaviour

- Terrorist attacks are often carefully planned and can include reconnaissance visits and dry runs prior to the selected day.
- It is vital that all staff remain alert to any unusual activity that may be taking place, especially if involving disgruntled former students.
- Report the activity immediately to the most senior member of staff available.
- Suspicious behaviour can manifest itself in a variety of ways:
    - Unusual questions about security measures, facilities and/or layout of rooms.
    - Close attention to entry/exits, stairwells, hallways and/or fire escapes.
    - Unusual movement of vehicles near buildings, structures and/or bridges.
- Suspicious behaviour is not always indicative of terrorist activity but may be an indicator of other criminal activity.
- This type of activity should always be reported.
- Never ignore your gut feeling. It is better that it is found to be bona fide behaviour as long as it is based upon what you honestly believed at the time.

Reporting it might just prevent an atrocity

Appendix 10

Telephone / Email Bomb Threat

If a telephone bomb threat is received, please refer to the following:

- **Bomb threat telephone calls:**
    - Make a note of the time of the call.
    - Let the caller finish. DO NOT interrupt them.
    - Stay calm and record exactly what the person says.
    - If possible use the bomb threat checklist for reference (see overleaf for this)
- **After the Call:**
    - Report the telephoned bomb threat to the police on **999** and then the most senior member of staff available. They will then provide an on-going point of contact for the police.
    - DO NOT cause the activation of any fire alarm.
    - Make yourself available for re-contact by the police either in person or by telephone.
- **Email or Social Media Threat:**
    - Do no reply, forward or delete the message
    - If email, note the address and print hard copy
    - If social media note which application has been used and any username / ID

Appendix 11

Bomb Threat Checklist

This checklist should be used in conjunction with the advice, to deal with a suspected telephone bomb threat:

Actions to be taken:

- Switch to tape/voicemail if connected.
- Tell the caller which town/district you are answering from.
- Record the exact wording of the threat:

……

Ask the following questions:

- **Where is the bomb right now?** ……
- **When is it going to explode?** ……
- **What does it look like?** ……..
- **What kind of bomb is it?** ……..

What will cause it to explode? ***Once the caller has hung up and the correct people have been informed:***

- **Time and date of the call:** ……
- **Length of the call:** ……..
- **Number that received the call:** ……..
- **Sex of caller:** ……
- **Nationality of caller:** ……..
- **Age of caller:** ……

Threat language:

- Irrational?
- Taped message?
- Offensive?
- Incoherent?
- Read by threat maker?

Callers Voice:

- Calm?
- Crying?
- Angry?
- Clearing throat?
- Angry?
- Nasal?
- Slurred?
- Excited?

Background Noises:

- Street Noise?
- Voices?
- Clear?
- Crockery?
- Music?
- Motor?
- Machinery?
- Office?
- Animal?

Any other remarks:

……
……

Print name:

……

Signature and date:

Appendix 12

Senior Member of Staff (Incident Coordinator) Bomb Threat and / or Suspect Bomb

If notified of a telephone bomb threat or a suspected bomb has been found, please refer to the following:

- **Bomb Threat:**
    - Ascertain as much information as possible from the person who took the call and take a number to re-contact them if necessary.
    - If the police are not already aware then telephone the police immediately with details and record their incident reference number.
    - The **INCIDENT COORDINATOR** should make themselves available as the point of contact for when the police arrive.
    - The **INCIDENT COORDINATOR** should arrange for a discreet search to be conducted by staff and security (if in attendance) in and around the building.
    - Before deciding upon an immediate evacuation the **INCIDENT COORDINATOR** should consider the context and details of the bomb threat and any advice the police can offer as to its likely veracity. Remember that an over-reaction may be exactly what a hoaxer is looking for and may encourage further calls.
- **Suspected Bomb Found:**
    - If as the result of a bomb threat search or otherwise an item deemed suspicious is found:
    - **DO NOT** handle the item, place it in water, cover it or tamper with it.
    - Try and discover its origin and obtain a description for the police, without touching it – In most cases the item will be readily identified.
    - **DO NOT** use mobile phone or radio within 15 metres of the suspect item.
    - The **INCIDENT COORDINATOR** should take into consideration the details of any verbal threat and also apply the “HOT” principles *(see red action sheet)* before deciding it is suspicious and implementing a course of action such as an evacuation (staff leaving a building or part of a building) or invacuation (staff moving to a safer part of the same building away from windows and behind solid cover).
    - The application of the “HOT” principles is vital to achieve a proportionate, safe response.
    - Should the suspect item be located next to the main exit or is outside the building it is often better to invacuate and not risk people passing close to it.
    - Inform the police of your action as soon as possible and tell them where you will be to meet them.
    - If you decide to evacuate **DO NOT ACTIVATE THE FIRE ALARM.**
    - Arrange for staff to be informed in a calm manner that there is a need to evacuate or invacuate and the reason why. Inform them of a safe route and where the assembly point is if leaving the building.

- Remember the assembly point should be beyond the following distances according to the size of the suspected bomb:
    - Small item up to briefcase size: **100 metres**
    - Large items up to and including car size: **200 metres**
    - Van or HGV size: **400 metres**
    - Be alert to secondary devices.
- If a letter or very small package a more limited evacuation is appropriate consisting of the room containing it, adjacent rooms (two in each direction from the device room). The same being applied to rooms two floors above and below the device.

Appendix 13

Indicators of Suspicious Mail

A delivered item will probably have received fairly rough handling in the post, so is unlikely to detonate through being moved. However, any attempt to open it, may set it off.

Unless delivered by courier, it is unlikely to contain a timer device. Items come in various shapes and sizes, but there may be tell-tale signs:

- It is unexpected and/or of an unusual origin.
- There is no return address or the address cannot be verified.
- It is poorly or inaccurately addressed.
- The address has been printed in an unusual way.
- The writing is in an unfamiliar style.
- There are unusual postmarks.
- A jiffy bag, or similar, has been used.
- It seems unusually heavy for the size. Most letters weigh up to about 28g (1 ounce), whereas most effective letter bombs weigh between 50-100g and are 5mm or more thick.
- It has more than the appropriate value of stamps.
- It is marked ‘personal’ or ‘confidential’.
- It is oddly shaped.
- The envelope flap is stuck down completely.
- There is a smell, particularly of marzipan or almonds.
- There is a pin sized hole in the envelope or wrapping.
- There is an additional inner envelope (however, this is common practice with some organisations sending restricted material).

Common and obvious chemical, biological or radiological (CBR) indicators:

- Unexpected granular, crystalline or powdered material (of any colour), loose or in a container.
- Unexpected sticky substances, sprays or vapours.
- Unexpected pieces of metal or plastic. e.g. disks, rods, small sheets or spheres.
- Strange smells. e.g. fish, fruit, garlic, mothballs, pepper. Some CBR materials are odourless and tasteless, however if you detect something, DO NOT continue sniffing it.
- Stains or dampness on the package.
- Sudden onset of illness and/or irritation of the skin, eyes or nose.
- CBR devices containing powder or liquid may be hazardous without being opened.

Appendix 14

IS THIS ITEM A SUSPECT BOMB?

"HOT" Principles

- **HIDDEN:**
    - Has the item been hidden?
    - Has any attempt been made to hide it from view or place it where discovery is unlikely?
    - Innocent items are not usually hidden.

- **OBVIOUS:**
    - Is the item obviously suspicious?
    - Does it look like a bomb?
    - Has it been found after a suspicious event?

- **TYPICAL:**
    - Is the item typical of what you might have found in the given location?
    - Example: Lost property is usually found where people gather or wait before moving on.

If confirmed as suspicious after applying the HOT principles and/or listening to the police, please refer to orange action cards