



# **Business Continuity Plan Guidance and Template to support the Department of Psychology**

## **Introduction**

The aim of this document is to help departments develop a response to prepare for and manage disruptive incidents.

Business Continuity Management sets out a framework and a process to enable you to plan the delivery of your departmental business during emergency events or lower level disruptions.

This process will help you to identify and manage risks and ensure you gather the information needed to build a simple Business Continuity Plan to protect your departmental business during a business disruption.

This document is divided in the three simple steps:

**Step 1** - Identify what your business products and or services and outputs are and identify which ones are the most important.

**Step 2** - Identify the risks that could prevent or interrupt your business from operating normally. At this stage it is a good idea to try and identify ways of protecting your business from these risks.

**Step 3** – Build your own Business Continuity Plan

## ► Step 1 - Business Products and Services

1. Document (in the table below) the products and/or services that your business produces or delivers.
2. Write a very brief description of each product or service.
3. Capture the key resources that you need to deliver the product or service. Think about the internal resources of your business first, such as staff, premises etc and then think about the external resources, such as suppliers next.
4. Finally, decide which are your most important products or services and number them, with '1' being the most important to your business and so on...

*\* This simple process should give you a good perspective on which products or services you need to think about protecting the most in order to ensure the survival of your department business.\**

Product or Service	Brief Description	Resources	Priority Order
<i>E.g.</i>	<i>See below</i>	<i>See below.</i>	
Teaching	Large (whole cohort) group lecturing	Lecture Theatre with demonstration facility. Staff. VLE.	1
	Large group practicals	Large PC lab. Staff. VLE. Specialist software.	2
	Small group teaching	Seminar rooms. Staff. VLE	3
Research	Instrument based research activity	Specific instruments	1
	Data analysis based research activity	Power, light, IT connection (remote), space. Staff	1
Service	MRI scanning to private paying patients	Specific instruments and location	4

## ► Step 2 – Identify Risks

It is important to consider risks that could impact on your department business and the measures that could be implemented to help reduce or manage the identified risks.

You should be able to identify risks from within your business, such as the work environment. However, you also need to try and identify risks outside of your business, such as the availability of key suppliers or impacts arising from severe weather.

You must decide what mitigation is appropriate and what is cost effective, based on the potential impacts.

Listed below are just a few simple examples of ways you can help manage the risk of disruption to your business:

### **a) Flooding/ Water damage**

- Are parts of the department susceptible to local ground water flooding
- Vulnerable to water leaks from upper floors?
- Local York flooding impact on travel and staff availability?

### **b) Interruption to energy supply**

- Is your department business particularly vulnerable to the possibility of the power supply being interrupted? If yes, what could it cost your business?

You could find that the impact could be significant and very costly...

- Are some items of research equipment vulnerable to power disruption?
- On the other hand, you may not be very vulnerable to energy interruption and it would only have minimal impacts. In which case you would not need necessarily to invest in measures to protect your business.

### **c) Loss of website or virus attack on key local IT systems**

- How big a risk would this be to your business? What would be the impact if this occurred?
- Consider how safe the information is that you hold locally and how sensitive it is.
- Are staff aware of what is backed up and what is not ?
- Consider sharing arrangements where appropriate with collaborators
- Impact on lectures, tutorials etc. if network ICT unavailable

### **d) Severe weather e.g. heavy snow**

- Consider the impact on staff and students accessing your department premises...what measures can you put in place to make access easier?

- What happens if your suppliers have difficulty delivering to you? How can you help staff prepare for travel into and from work?

### e) Fire Risk

- Consider if your business premises is at risk of fire.
- For example, are highly flammable materials/goods stored within the premises, are they correctly stored?
- Are there tools or equipment on site that could cause fire, if so are they well maintained?
- What about neighboring business and properties? Could they cause an increased risk of fire?
- Are your evacuation plans and fire detection equipment appropriate and well maintained?
- Are all your staff trained in what to do in a fire and ensure customers and visitors are evacuated safely in case of a fire?

\* The above details some of the threats to your business, but you are best placed to understand the specific risks to your business and the potential impact that they would have if they occur.\*

*\* The above details some of the threats to your business, but you are best placed to understand the specific risks to your business and the potential impact that they would have if they occur.\**

Possible Impact	Possible Risk	Possible Prevention	Possible Solution
<b>Workspace loss or inaccessible</b>	Fire	Fire alarm, fire fighting equipment, staff and student training.	Work from alternative location?
	Loss of electrical power	PAT testing, see DECS Business Continuity Plan	See DECS BCP
<b>Loss of Staff</b>	Severe Weather e.g. heavy snow	Receiving 'Weather Warnings' triggering communication with staff, and suppliers.	Arrange suitable lecture small group activities Work from home? Ensure sufficient staff on site to continue teaching work. Ensure sufficient staff on site for safe operation of all areas
	Sickness		Temporary cover for some activities
	Travel disruption e.g. RTC local flooding	Encourage sustainable transport practices	Work from home/alternative accommodation
<b>Loss of IT &amp; Data</b>	IT Virus	Anti-Virus software kept up to date.	Safely backing up data.
	Network outage	See IT Services BCP	Local copies of resources. See IT Services BCP

	Physical damage to infrastructure	Major works carried out through Estates	See IT Services BCP
<b>Loss of specific instruments of equipment, affecting service to patients</b>	Fire or flood	Fire Alarms, staff training	Initial suspension of service. Service is provided to non-urgent issues and alternative local services exist.
<b>Loss of Other Resources</b>	Loss of water		
	Loss of heating		

**\* Remember to store copies of key documents, contracts and business credit or debit cards etc safely and securely off-site in case your premises are damaged or you lose access to them**

## ► Step 3 - Build your Business Continuity Plan

### Advice for completing the plan template...

The following template is just a simple plan outline to help you protect your department business.

It is designed to help you capture important actions that you or your staff would need to undertake should there be a business disruption.

The text in *italic* is there to illustrate some examples of the type of actions that you may want to consider when you develop your plan. You can build from this and make it specific to your business.

**\* Once completed, the plan should be stored securely off-site and be accessible to those that would need to implement it...remember that key documents such as contact documents, client information, contracts and supplier details should also be stored securely off site. It is also a good idea to have a business debit or credit card away from your business premises just in case you cannot access your work environment. \***

# Department of Psychology

## Business Continuity Plan

<b>Version Number:</b>	1
<b>Plan Owner:</b>	Nicole Warmus
<b>Date Published:</b>	November 2017



# Contents

Section	Content	Page
<b>1.0</b>	<b>Staff Contact List</b>	
<b>2.0</b>	<b>Your Business Priorities</b>	
<b>3.0</b>	<b>Plan Activation Procedures</b>	
3.1	Plan Activation Process	
3.2	Managing loss of Workspace	
3.3	Managing loss of IT / Data	
3.4	Managing loss of Key Staff	
3.5	Other Resources	
<b>4.0</b>	<b>Supporting Information</b>	
4.1	Staff Welfare	
4.2	Communicating With Staff	
4.3	Media / Public Information	
<b>5.0</b>	<b>Plan Maintenance Procedures</b>	
<b>Appendix</b>	<b>Other Useful Numbers</b>	

Plan Distribution List			
	Name	Role	Issue
1	Mike Burton	HoD	
2	Tim Andrews	Deputy HoD	
3	Shirley-Ann Rueschemeyer	Chair of BoS	
4	Garry Turner	Technical Manager	
5	Tony Morland	Director of YNiC	Issues affecting YNiC
6	Nicole Warmus	Department Manager	
7	Martyn Godwin	Business Continuity Champion, HSSD	
8	Elizabeth Meins	Chair of Departmental Research Committee	

# 1.0 Staff Contact List

**If there is ever a business disruption or emergency call the main on-call number as soon as you can which is the Security Control Room: 01904 32 3333**

Departmental Incident Response Team (DIRT)

## Emergency Contacts List

Please work down the list in order of priority:

Name	Job Title	Telephone Numbers			Call Out Categories
		Work	Home	Mobile	
Mike Burton	Head of Department	3140			<ul style="list-style-type: none"> <li>Emergencies, business continuity concerns for all Department, staff and students</li> </ul>
Tim Andrews	Deputy Head of Department	4356			
Nicole Warmus	Department Manager	3178			<ul style="list-style-type: none"> <li>Emergencies, business continuity concerns for all Department</li> </ul>
Garry Turner	Technical Manager	2870			<ul style="list-style-type: none"> <li>Business continuity concerns regarding IT</li> </ul>
Shirley-Ann Rueschemeyer	Chair of Board of Studies	2885			<ul style="list-style-type: none"> <li>Business continuity concerns regarding students and teaching provision</li> </ul>
Antony Morland	Director of YNiC	2860			<ul style="list-style-type: none"> <li>Emergencies, business continuity concerns for York Neuroimaging Centre</li> </ul>
Elizabeth Meins	Chair of Research Committee	4602			<ul style="list-style-type: none"> <li>Business continuity concerns regarding research facilities</li> </ul>

## 2.0 Your D Priorities

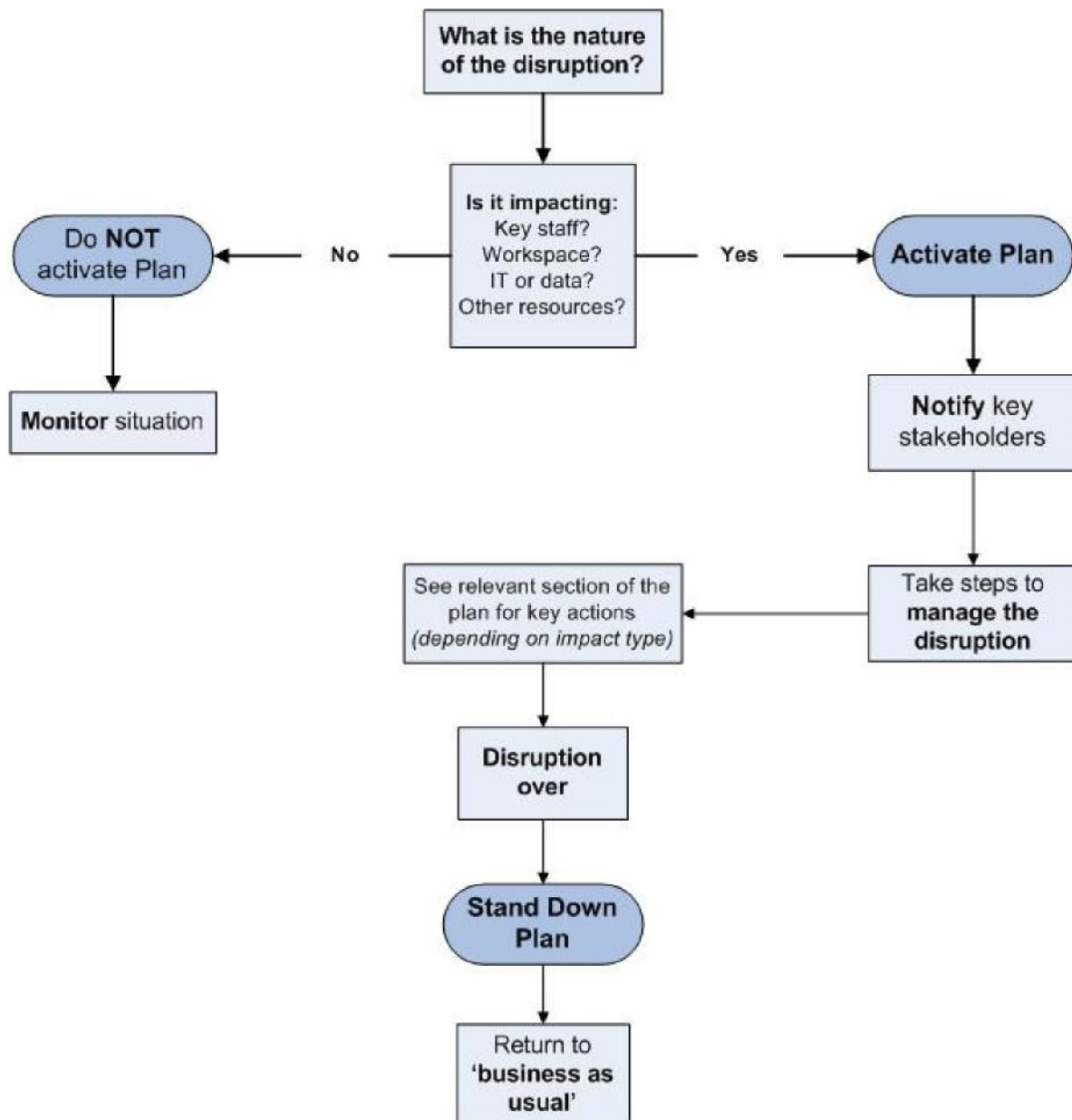
\* Add the services / products that you identified in step 1 into the table below \*

PRIORITY	SERVICE / PRODUCT
1	Large (whole cohort) group lecturing
2	Instrument based research activity
3	Data analysis based research activity
4	Large group practicals
5	Small group teaching
6	Service for paying patients

**\* It is important to ensure suppliers that support your business priorities have robust business continuity arrangements. If they do not have robust arrangements consider how you would manage knock on impacts to your business and what you need to do to protect your business.\***

## 3.0 Plan Activation Procedures

### 3.1 Plan Activation Process



## 3.2 Workspace

Objective	Actions or Considerations
<b>Establish the current situation at the affected site or workspace.</b>	<ul style="list-style-type: none"> <li>• What has happened?</li> <li>• When did it occur?</li> <li>• Are the Emergency Services informed or on-site?</li> <li>• Is there access to the site?</li> <li>• Are the IT systems and services still running?</li> <li>• Who else has been informed?</li> <li>• How potentially serious is it?</li> <li>• Are there any casualties? If so, details?</li> </ul>
<b>Decide whether to invoke Business Continuity plan.</b>	<p>The decision will be based upon the information provided consideration should be given to:</p> <ul style="list-style-type: none"> <li>• How quickly the business will be able to re-enter the affected workspace?</li> <li>• Prevailing weather conditions.</li> <li>• Whether the area is currently responding to an external incident.</li> <li>• If the decision is made not to invoke the plan, continue to monitor the situation until such time as normal access is granted to the disrupted location.</li> </ul>
<b>Communicate with staff, suppliers or customers.</b>	<ul style="list-style-type: none"> <li>• IF EVACUATION IS NEEDED: follow site evacuation plan taking into account staff, customer and visitor safety.</li> <li>• Keep staff informed at Assembly Points until a decision has been made about whether the building is likely to become available again soon. If the building will not be available, relocate identified key staff to the agreed alternative workspace and consider sending other staff home and tell them to await instructions. Remind them to check in with their manager at an agreed time.</li> <li>• Out of Hours: if the disruption occurs outside office hours, staff communication will be co-ordinated by the Departmental Response Team.</li> <li>• Communicate with staff and students.</li> </ul>

### 3.3 IT Systems / Data

Objective	Actions / Considerations
<b>Confirm the nature of the disruption.</b>	<ul style="list-style-type: none"> <li>• What has happened?</li> <li>• When did it occur?</li> <li>• Which systems and/or services are affected?</li> <li>• How potentially serious is it?</li> <li>• What is the estimated duration of the problem?</li> <li>• Who else has been informed (staff/ suppliers /</li> </ul>
<b>Decide whether to invoke Business Continuity plan.</b>	<p>The decision will be based upon the information provided consideration should be given to:</p> <ul style="list-style-type: none"> <li>• How long systems will be unavailable?</li> <li>• Whether the systems affected are required to support the business priorities?</li> <li>• Whether the area is currently responding to an external incident?</li> <li>• Inform staff that the Business Continuity Plan is being invoked <b>or</b> put staff on standby <b>or</b> invoke agreed manual systems to ensure that the service can continue to operate.</li> <li>• If the decision is made not to invoke the plan, continue to monitor the situation until such time as normal service is resumed.</li> </ul>
<b>Enter specific actions or considerations if the disruption is due to non- availability of IT systems or Data.</b>	<p>Some examples of solutions / strategies:</p> <ul style="list-style-type: none"> <li>• Instigate manual work around systems</li> <li>• Close liaison with IT Services</li> <li>• Accessing and making available critical data to key staff which has been protected.</li> <li>• Working from a secondary location on campus unaffected by the IT issue.</li> <li>• Communicate with staff and students.</li> </ul>

### 3.4 Key Staff

Objectives	Actions / Considerations
<b>Confirm the nature of the disruption</b>	<ul style="list-style-type: none"> <li>• What has happened?</li> <li>• When did it occur?</li> <li>• Who and how many are affected?</li> <li>• Which systems and/or services are affected</li> <li>• How potentially serious is it?</li> <li>• What is the estimated duration of the problem?</li> <li>• Who else has been informed (staff / students / suppliers /customers)</li> </ul>
<b>Decide whether to invoke Business Continuity plan.</b>	<p>The decision will be based upon the information provided consideration should be given to:</p> <ul style="list-style-type: none"> <li>• How long staff will be unavailable</li> <li>• Whether the staff are required to support the business priorities.</li> <li>• Whether the area is currently responding to external incident</li> <li>• Inform staff that the Business Continuity Plan is being invoked <b>or</b> put staff on standby <b>or</b> invoke agreed manual systems to ensure that the service can continue to operate.</li> <li>• If the decision is made not to invoke the plan, continue to monitor the situation until such time as normal service is resumed.</li> </ul>
<b>Enter Specific actions or considerations if the disruption is due to non- availability of Staff.</b>	<ul style="list-style-type: none"> <li>• Change of job functions for some staff (to support the business priorities e.g. assisting with teaching activities)</li> <li>• Offer overtime</li> <li>• Rearrange teaching where possible</li> <li>• Communicate with staff and students.</li> </ul>

### 3.5 Other Resources

Objectives	Actions / Considerations
<b>Confirm the nature of the disruption</b>	<ul style="list-style-type: none"> <li>• What has happened?</li> <li>• When did it occur?</li> <li>• Which systems and/or services are affected</li> <li>• How potentially serious is it?</li> <li>• What is the estimated duration of the problem?</li> <li>• Who else has been informed? (staff / students /suppliers / customers)</li> </ul>
<b>Decide whether the Business Continuity Management Plan should be invoked.</b>	<p>The decision will be based upon the information provided consideration should be given to:</p> <ul style="list-style-type: none"> <li>• How long resources will be unavailable</li> <li>• Whether the resources affected are required to support the business priorities?</li> <li>• Whether the area is currently responding to an external incident?</li> <li>• Inform staff that the Business Continuity Plan is being invoked <b>or</b> put staff on standby <b>or</b> invoke agreed manual systems to ensure that the service can continue to operate.</li> <li>• If the decision is made not to invoke the plan, continue to monitor the situation until such time as normal service is resumed.</li> </ul>
<b>Enter Specific actions or considerations if the disruption is due to non-availability of resources.</b>	<ul style="list-style-type: none"> <li>• Arrangements/contracts to hire / borrow / purchase replacement resources from suppliers.</li> <li>• Assess if loss of other resources (such as energy or water supply) results in loss of work space and if so, see 3.2.</li> </ul>



## **4.0 Supporting Information**

### **4.1 Staff Welfare**

Staff need to be given clear direction about what the priorities of the business are, this can be achieved by having well thought out continuity strategies in place. Ensure that you monitor staff more closely to ensure that their welfare is maintained (e.g. regular breaks due to increased intensity or pressure of work, and support in case their normal duties change).

Staff must be made aware of what communication methods are going to be used so they can find out the latest information, especially if they are going to be working from home or a different location than normal. If staff are going to be working from a different location, ensure that they know where the location is (provide a map and or directions if necessary) and they are able to get there and get access.

### **4.2 Communicating with Staff**

#### **\*Out of office hours\***

The Departmental Response Team will keep staff up to date by the following methods:

- Telephoning staff and passing on essential information.
- Mobile phone text cascade of information if appropriate.
- Via the communications team

Information may be available via the following depending on the reason for disruption: Departmental Wiki.

Staff should be given the opportunity to feedback any comments they may have after the response phase and the service has returned to normal. This may be in the form of a structured debrief or more informally.

Managers who suspect that staff members have suffered undue stress or even trauma from the business disruption must consider providing assistance for those staff that have been affected.

### **4.3 Communicating with students**

In the event of a major disruption students the Departmental Response Team will liaise with the central Timetabling team and/or central student services team, who have means to contact students by text.

### **4.4 Media / Public Information**

In the event of a major disruption to the Department the Major Incident Response Team must be contacted to inform them of what has happened and the estimated length of the disruption and possible impacts of the disruption.

## **5.0 Plan Maintenance Procedures**

Review contact lists every 6 months and review the whole plan annually. Carry out a test during a meeting to test the Business Continuity Plan works and your staff understand arrangements.

## Appendix A

A staff contact list is held confidentially by the Departmental Incident Response Team and is maintained by the departmental HR team.