

# Business continuity

*...and your school*



July 2021

## What it is...



## Why plan?

*“Business Continuity management is when an organisation identifies risks that may interfere with delivery of products or services and puts in place plans to mitigate interruptions to enable return to usual business quickly and with as little disruption as possible”*

Schools, like other organisations, may face disruptions caused by critical incidents. Creating an effective **Business Continuity Plan** will help you build resilience to get your school back on track faster, reducing impact on pupils, staff and parents.

A plan will help you to understand your learning environment and empower staff to react effectively to overcome any challenges.

It also means you will have all the important information you need during and following an incident (such as contact details and action cards).

You will be able to respond and recover more effectively and efficiently, keeping financial losses to a minimum.

It means supporting your pupils, your staff, your parents, your reputation and your key activities.

Whatever the size of your organisation, planning is the most effective way to overcome any incidents you may face.

Your plan will allow you to identify the critical activities, what threats you may face and identify some mitigation strategies in case something does go wrong.

## Why plan?



# Planning

Business Continuity	Yes	No	Don't Know
Has the idea of Business Continuity Management (BCM) been agreed at Governor/Management level?			
Do you have a Business Continuity Plan (BCP)?			
If yes, is the plan documented clearly and easily accessible?			
Have you exercised your plan within the last 12 months?			
Is there a policy for how and when to activate the plan?			
Do you regularly review and update the plan?			
Are staff trained in activating and operating the plan?			
Who in your organisation will have responsibility for looking after Business Continuity?			
Have you made a list of key contact telephone numbers?			
Have you prepared an emergency pack?			

## Include within your plan:

- ✓ Introduction
- ✓ Aims and objectives
- ✓ Key critical activities list, with their critical time frames (how long can you cope before getting each activity started again)
- ✓ Known potential risks and threats
- ✓ Plan triggers
- ✓ Activation process
- ✓ Action cards for response
- ✓ Recovery process
- ✓ Key contacts, customers, suppliers, staff, other stakeholders

How you plan for and respond to events such as fire, flooding, vandalism or loss of utilities, for example, can determine how quickly and to what level your organisation can recover.



Adverse weather



# Key impacts and considerations

IT failure, equipment and stock



Flood



How would you continue in the event of an incident? Think about:

- Premises – loss of or inability to access. Could you “buddy” up with a nearby school to help one another if an incident occurs?
- People – loss of staff or skills. Safety, wellbeing, welfare
- Communications – staff, suppliers, customers, media
- Equipment / stock – loss of key suppliers, supplies or utility supplies, loss of key or specialist equipment
- Computers, network access and telecoms – interruption to or loss of
- Financial issues
- Transport disruption
- Sources of help and advice

Power Outage



Staff and skills



Media and Comms



Pandemic



Fire



## Key impacts and considerations 2

### What are the critical activities?

- What services do you provide?
- Do you have any statutory responsibilities?
- Are there any legal or financial implications if your product/service is impacted?
- What are the priorities of these activities?

### For each critical activity:

- What is the priority?
- How long could you cope without that activity?
- What difficulties might you face?

### What would the impact be if interruption lasted for:

- 24 hours
- 24-48 hours
- Up to 1 week
- Up to 2 weeks
- Longer than a month

If you or your organisation are involved in an incident and believe you may be in danger always dial **999** to request the appropriate emergency assistance.

If you are not in danger but may be affected indirectly, you may be advised to **GO IN, STAY IN, TUNE IN**

## Starting your plan

**Keep it simple.** It's just a matter of assessing risks, keeping useful information to hand in case of an incident (big or small), keeping the information up to date, practicing and learning any lessons from incidents you may have already encountered. Give some thought to the following:

- Assessment of impacts and risks
- What is critical to deliver services?
- Supply chain – alternatives if supply interrupted, key contacts
- Restoring key processes – how, who, where, resources?
- Safeguarding
- Communication – staff, media, suppliers, stakeholders, up to date contact details
- Health and safety
- Staff welfare
- Keeping plan information up to date



# Six steps to plan

“Business Continuity is a holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities”

**Business Continuity Institute**



## 1 Know your organisation

- What is the aim of the organisation and what are the key activities involved in achieving it?
- What resources do you need for the key activities to happen? Think about staff, premises equipment, communication, links, IT, suppliers, specific knowledge or training.
- What deadlines to you work to?

## 2 Assess the risk

- What risks could your organisation face?
- What critical activities might be impacted?

# What's critical, what's not?

## 3 Develop a strategy

- What actions will you take if an incident happens?
- How will those actions be done?
- Who will do these actions?
- Where will the actions take place? On site or at an alternative location?
- What will the priorities be?

## 4 Write your plan

- Use the information you have gathered to write the plan
- Templates with guidance notes can be found [here](#)

## 5 Test your plan

- You should test your plan by carrying out an exercise to see if your assumptions work.
- Staff must become familiar with it and have an idea of what would happen in a real incident.
- Some scenarios to help you are included within this booklet.

## 6 Maintain your plan

- Review your plan on a regular basis
- An out of date plan could be almost useless when you actually need it

# Plan considerations - checklist

**This is not an exhaustive list but aims to help you.** Capture any details in your plan where you have answered Yes. If you have selected No or Don't Know, consider whether these are relevant to your organisation.

Equipment, Data and Documentation	Yes	No	Don't Know
What is your key equipment?			
Is there contingency plans in place to cater for the loss or failure of key equipment?			
Do you regularly update an inventory of key equipment for your organisation?			
Do you have any controls for the movement of your equipment?			
Do you regularly copy/back-up data and information?			
Are critical documents protected robustly?			
Do you have copies of critical records at a separate location?			

## Plan considerations – checklist 2

Buildings and People	Yes	No	Don't Know
Does your premises have an emergency evacuation procedure? Are there fire safety procedures in place?			
Do you have access to the premises at all times?			
If yes, is the plan documented clearly and easily accessible?			
Do you have access to an alternative workplace to use in an emergency?			
Do you have a list of all employee contact telephone numbers and home addresses? Where is this stored?			
Have staff been allocated specific roles in the event of an incident?			
If the premises was made unavailable, could staff work from an alternative location or from home?			
Are any staff members proficient in first aid or have medical training?			
Have you identified or considered any risks to your organisation from the surrounding area or other businesses, eg Flood risk?			

# Plan considerations – checklist 3

IT	Yes	No	Don't Know
Are your IT systems critical to the running of your organisation?			
If the IT system was inaccessible are there manual processes that could maintain critical functions and administration?			
How long would IT recovery take?			
Who would recover the system? What are their contact details?			
Do you have a tested IT disaster recovery plan?			
Is your computer anti-virus software up to date?			
Are documented IT security policies and procedures in place? Are all users fully aware of e-mail and internet usage policies?			
Is your company system part of a larger network?			
Do you know how many platforms/services/applications or operating systems support critical functions?			
Is expertise of how to use your IT system, knowledge of where critical documents are electronically stored etc, limited to one individual?			
Do you have vital computer information stored on back-up discs held off site?			

# Plan considerations – checklist 4

Customers and Suppliers	Yes	No	Don't Know
Do you have alternative suppliers for critical equipment/ stores/ parts/goods/ products etc?			
Do you have an arrangement with your critical suppliers where they will inform you if they cannot make a delivery?			
Do your suppliers have a business continuity plan?			
Do you have your suppliers correct contact details both office hours and out of office hours?			
Do you have the correct contact details for all your main customers?			
Do you have any key customers who you will need to be in constant contact with during a crisis?			
<b>Other</b>			

## Scenario: loss of staff

### Consider

- Who are the key members of staff?
- Can staff work at alternative locations?
- Do other staff members know and understand how to do key activities?
- How will you communicate with staff?
- Where are staff based in relation to your workplace?

### What are your next steps?

- Ensure all staff are trained in key roles
- Re-task staff from non-essential roles
- Consider use of agency staff or contractors
- Postpone any non essential activities
- Consider outsourcing activities where applicable
- Ensure all staff contact details are up to date

## Exercise 1

This scenario means that supporting staff resources are affected because of contagious illness, strike, transport, outrage, adverse weather etc **Remember to update your plan with any lessons learned from this exercise.**

### Questions

1. What are the immediate effects of this incident on the ability of your organisation to operate as usual? What immediate actions are required?
2. How will you minimise the impact on your critical activities?
3. What staff welfare responsibilities do you have?
4. What workaround options in this scenario do you have, especially for the most essential services you provide?
5. How will communication continue with staff, customers, relatives or others? Where do you keep contact details?
6. What further contingency arrangements need to be considered?

**We are here to help...**



**when you need it**

**Children's Services Incident Management Team**  
- here to assist you if an incident occurs -

**IF YOU ARE CURRENTLY DEALING WITH AN  
INCIDENT PLEASE CONTACT: -**

**COMMUNITY ALARM CENTRE (CAC)**  
**Tel: 01908 226699 (24 hrs)**

**AND QUOTE CODE**

**"Children's Services Incident Management Team"**

School has critical incident, requires support or needs to alert Milton Keynes Council (MKC)

School phones CAC (keep contact info in contact section of BCP or available on MKC website)

School gives CAC the code – "Children's Services Incident Management Team"

CAC advises school that the CS IMT will be alerted

CAC advises CS IMT and relevant Director (if out of hours by mobile) and recounts information

CS IMT Chair will respond and invoke CS IMT if required

# Guides

## MKC templates and appendices for schools

Further advice and templates can also be found at: -

- [The government business continuity Toolkit](#)
- [The Business Continuity Institute \(BCI\)](#)
- [BCI Good Practice Guidelines a step by step guidance document](#)

# Emergency Pack Contents

If you had to evacuate in an emergency, having some key details at hand or stored off-site could make a significant difference in how quickly you can react.

Your emergency pack could contain:

- ✓ Business continuity plan (BCP)
- ✓ Contact details for insurance, customers, suppliers, landlord etc to be contained in the BCP
- ✓ Spare copies of BCP appendices, log sheets, contact lists etc
- ✓ Building plans (if appropriate)
- ✓ Laminated action cards
- ✓ High visibility vests
- ✓ Salvage inventory
- ✓ Basic toolkit
- ✓ Phone chargers
- ✓ Pen and paper to write down anything important



**Contact us:**

**E: [businessresilience@milton-keynes.gov.uk](mailto:businessresilience@milton-keynes.gov.uk)**

**T: 01908 253312**

**Civic, 1 Saxon Gate East, Milton Keynes MK9 1EJ**



**milton keynes council**

