GIPPESWYK COMMUNITY EDUCATIONAL TRUST

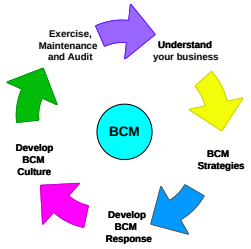
This Policy has been adopted and approved by Gippeswyk Community Educational Trust and is to be used by all members of the Trust.

BUSINESS CONTINUITY MANAGEMENT POLICY	
Approved by GCET	06.03.2018
Date of next Review	Summer Term 2020-2021 *(Two yearly – even years)*
Responsible Officer	Trust CFO – Mrs T Goodchild
Policy Number	TF5

Table of Contents

1 INTRODUCTION

1.1 Purpose



This Business Continuity Management (BCM) Policy defines the process within which the Academy can set up activities for establishing a business continuity capability and its ongoing management and maintenance.

1.2 Overview

BCM involves managing the recovery or continuation of business activities in the event of a business disruption. Maintenance is a continuing, cyclic activity that ensures the business continuity plans stay current and up to date through training, exercises and reviews.

2 THE POLICY

The BCM programme will meet the following objectives:

2.1 Understanding the organisation

- A business impact analysis (BIA) will be carried out to identify the key products and services and the critical activities and resources that support them.
- Impacts of disruption will be assessed to establish the maximum tolerable outage (MTO) that critical activities can withstand.
- A set of risks to the business will be identified which could lead to a business disruption, loss, emergency or crisis.

2.2 Determining the business continuity strategy

- Information gathered from the BIA will be used to determine the Academy's corporate response to an incident.
- Strategies may depend on the nature of the incident, the MTO of critical activities, the cost of implementing the strategy and the consequences of inaction.
- Mitigation strategies will be implemented to reduce the likelihood of incidents occurring and/or reduce the potential effects of an incident.

2.3 BCM Response

- GCET (all members of GCET) will use the business continuity strategy and the BIA information to develop plans covering:
    - Corporate crisis management.
    - Operational incident management.
    - Business Continuity Plans (BCP) at team level.
    - Business resumption.

2.4 Culture

- All staff should undertake awareness and skills training.
- BCM should be incorporated within change management to ensure it is kept up to date and relevant to the activities of the organisation.
- All staff are encouraged to provide their managers or team leaders with contact details which can be used to provide them with information, or to request their assistance, in the event of an emergency affecting the Academy.

2.5 Exercise, maintain, audit

- All plans will be subject to regular exercises.
- All plans must be reviewed at least annually.
- The BIA should be reviewed annually

- External auditing of the BCM programme should be carried out every 2 to 3 years to ensure compliance with industry best practice.

3 SCOPE

3.1 BCM Programme management

The programme will be managed by the Principal.
The programme will be guided by BS25999-1 Business Continuity Management – Part 1, Code of Practice.

3.2 Application

This policy applies to:

3.2.1 Staff

- All staff employed by or seconded to GCET.

3.2.2 Premises

Copleston High School
Rose Hill Primary School

3.2.3 Technology

- All ICT systems maintained on behalf of the GCET.
- All telephone systems maintained on behalf of the GCET.
- All ICT systems solely used by the GCET.
- All network systems maintained on behalf of the GCET.

3.2.4 Information

- Physical formats, i.e. hardcopies such as paper or microfilm
- Electronic formats, i.e. computer files including backups

3.2.5 Suppliers:

- Suppliers of essential services should be required to provide evidence of their business continuity readiness.
- New contracts with potential suppliers should require evidence of their business continuity readiness.

3.3 Overriding considerations

- The health and safety of all affected persons must be safeguarded at all times.
- All UK regulations must be fully adhered to, including specifically the Civil Contingencies Act 2004 and Data Protection Act.
- Academy staff must be able to respond in a practised manner.
- Our customers' requirements must be met and liaison with them must be efficient and accurate.

4 CONSTRAINTS

- Constituted as a charitable company limited by guarantee, the GCET must comply with company law as set out in the Companies Act 2006 (and subsequent Acts) and charity law and the requirements of the Charity Commission.
- The Academy is also subject to the terms of the Funding Agreement with the Department for Education and must abide by the provisions within the Financial Handbook.

5 GLOSSARY

Term	Definition
BCM	**Business Continuity Management** is a holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.
BIA	**Business Impact Analysis** is the process of analysing business functions and the effect that a business disruption might have on them.
GCET	The **GCET**, including all employees, trustees and governors.
Incident	A business continuity **incident** is a situation that might be, or could lead to, a business disruption, loss, emergency or crisis.
MTO	**Maximum Tolerable Outage** is an estimate of how long it would be before the loss of a function starts to affect the company or customer operations.

Appendix A

Business Continuity Plan
ICT Department

The ICT Department manages the school network and telecoms. The main server room is located in the centre of the school, next to B100, and contains all of the school's servers, main switch, router and telephone modules (PABX and voicemail server).

Schools emails have been migrated to Office 365/Exchange Online for increased resilience in the event of server outage on site.

The broadband line is an uncontended direct to site line with BT Business with failover in the event of an outage.

Telecoms Failure

The school telecoms system is managed by Excell. In the event of a service failure, we will contact Excell and ask them to investigate the fault. If external lines are down, we arrange to have the main school telephone number diverted to a school mobile until the problem has been resolved. The First aid office is also given a school mobile in case they need to contact parents in an emergency.
Excell will work with BT Openreach to solve any problems with external lines. Once the problem has been resolved, the diversion is removed and the school phones will function as normal.

In the event of a hardware failure, we would contact Excell and arrange to have an engineer visit the site as soon as possible.

In the event of a fire (in the server room) then we would need to contact Excell to assess the damage and replace any equipment as required. Most of our phones are VoIP (Voice over IP) and connect via the school network. Therefore, we would to restore connectivity from the main switch before the phones would be functional.

Network Failure

The school network contains several switch cabinets for connecting PCs and other devices in each area of the school. Each switch cabinet contains one or two switches (depending on load). We have a fibre backbone to most areas of the school. Short "hops" between switch cabinets are serviced by Cat5e cabling.

In the event of a switch failure, we always keep at least one spare 48 port switch on site. This allows us to quickly swap the faulty switch out and restore connectivity to the affected area as soon as possible.
If a switch cabinet is damaged by fire or other disaster, we would liaise with a company such as Inviron to assess the electrical damage. Once power is restored to the area, we would work with Inviron to rewire the affected switch cabinet as required.

We have redundant links to switch cabinets so that if a link in one area should fail, data can still be sent to and from that switch cabinet using the second link.

Servers/SAN/Backup

We are currently running three servers which host Virtual Machines. These three servers are connected to a SAN via an iSCSI link. We have two switches connecting the SAN to the servers and use MPIO so that if one switch fails the SAN and servers can still communicate.

The three host servers are connected in a failover cluster environment. This means if one server fails then the services and virtual machines that were running on that server will automatically failover to one of the other servers. This happens automatically as soon as the other servers detect the third is no longer available.

The SAN itself is configured in a RAID 6 and 10 array. The two separate SAN shelves are configured with RAID 6 and the whole SAN (clustered) is configured with RAID 10. This allows maximum redundancy for the hard drives in the SAN. Both shelves have a dedicated hot spare hard-drive. If one drive fails, the spare will be used automatically. We have a 4-hour response time warranty with HP so the failed hard drive will be quickly replaced- either same day or next day.

Backups are managed by Redstor. This is an offsite backup company with two data centres- one in Reading and one in Slough. Backups of all servers are encrypted and sent to Redstor every evening. This data is duplicated to their second data centre. We also have a duplicate copy kept onsite in case the internet connection fails.

If a server fails and the problem could not be resolved, we would reinstall the Operating System. We would then restore the latest backup data from Redstor.

If there was an issue where hardware was damaged in the server room (e.g fire/flood etc), we would need to obtain new equipment from suppliers as soon as possible. We don't have redundant servers in place and do not have a contact with a company who can provide hot spares due to cost. There would obviously be some downtime caused by this as it would depend on how quickly we could secure the funds required for the amount of equipment needed. Once replacement equipment is in place, we can restore data from Redstor backups.