Business Continuity Plan

Version	0.1
Approved By	Trustee Board
Issue Date	30 June 2022
Last Review Date	September 2023
Next Review Date	September 2024

REVIEW HISTORY

VERSION NO.	DATE OF CHANGE	CHANGE SUMMARY	REF.
0.1	24.2.2022	New draft	
2.0	5.7.2023	Added Appendix 6 – action plan	20
		Preventative Strategies	6

Table of Contents

Introduction

Oak Multi Academy Trust's central team (The Trust) is exposed to events which have the potential to cause major disruption to our services. Although such events are rare, it is important that we have in place plans to help us manage and recover from these situations as they arise. Not only is this good practice, but it is also considered essential for an organisation responsible for delivering high quality education to the community.

One of the problems in planning for a disruption event is that it is impossible to predict what that event might be or when it might happen. In developing these plans, we need to be mindful of any particular vulnerabilities or risks to which our Trust is exposed.

Rather than developing many plans to deal with every foreseeable eventuality, our plan is structured around the concept of failure or loss of access to the key resources we need to provide our services.

This means, irrespective of the cause, our plan focuses upon the loss of data, IT and communication systems, office workspaces and facilities, and our human resources. In this way, regardless of whether the adverse event is a major fire, a bomb, or a flu epidemic, we have plans in place to effectively manage the loss of the affected resource.

The Trust Business Continuity Plan (BCP) has been written for those who will be involved in re-establishing the operational delivery of services following a major incident or crisis. It should be read in conjunction with:

- Each individual school's Business Continuity Plans within the MAT
- Each school's fire evacuation plan (the operation of which does not necessarily activate the BCP).
- Each individual ICT Disaster Recovery Plan, where appropriate.
- Safeguarding and Child Protection Policy
- The Risk Management Policy and the Risk Register

This document sets out the Trust's approach for planning and responding to major incidents which affect the continuity of the Trust's business and the safety of its staff, pupils, and others. **In the event of a major disaster which affects all schools within the Trust, each school is expected to invoke its Business Continuity Plan.**

This document should be reviewed annually by the CEO and the Board of Trustees.

School Business Continuity Plans

Wherever possible, all schools should unify the template used for the creation of the Business Continuity Plan to make it easier to identify gaps or common approaches across each school within the Trust. This will also make the review of the BCP's for all schools much easier. Each school must ensure that their business continuity planning is informed by a risk assessment of critical activities to identify key risks specific to its operation and the safety of its pupils, staff, and others. This assessment will be led by the Headteacher.

As a minimum, there must be specific plans in place for ICT Disaster Recovery & Alternative Temporary Premises. Each school will maintain its own Emergency Management Instructions; including emergency contact details, call cascade plan and the action plan. The cascade plan must be tested on an annual basis.

Definitions

The recovery objectives and priorities of this plan are based upon the nature of our business and have been developed in direct accordance with the results of a service impact analysis. The service impact analysis was conducted to provide a specific insight into the criticality of the different components of the Trust, and to ensure that our response to an adverse event which may affect continuity is efficient, effective and is focused entirely in accordance with the needs of the Trust.

A disaster is the escalation of an emergency to the point where normal conditions are not expected to be recovered for at least 24 hours.

Severity of incidents

Minor Incidents

These are events or circumstances that the Trust can deal with using its built-in procedures which does not affect the Trust adversely or prevent it from carrying out its day-to-day activities.

Major Incidents

These are events or circumstances that cause or threaten death or injury, disruption to the Trust and is on such a scale that it prevents the Trust from carrying out its day-to-day activities. All these types of incidents would be handled by the school's Business Continuity Plans and must be notified immediately to the CEO. An Incident Management team would be established to support the Headteacher of the school to implement all the actions.

Crisis Management

An initial assessment of the incident by the CEO will establish if the incident should be handled as a Major Incident or whether a Crisis should be declared. A crisis would typically be an event that impacts multiple schools within the Trust or has the potential to threaten the future operation of the Trust. An Incident Management Team (IMT) will be established at the declaration of a crisis to assist the Trust in managing the response. The membership of the IMT may vary slightly depending on the nature of the incident as different skills will be required depending on the nature of the incident but will always be chaired by the CEO.

Strategy

If a crisis is declared that is localised to within one school, then this can be declared by the school's Headteacher or their deputy and their own BCP invoked. Any crisis declared must be immediately notified to the CEO. This notification process must be embedded within each school's Business Continuity Plan.

If a crisis is declared within the Trust central team or there is trust wide impact, then the Trust Business Continuity Plan will be activated.

Incident log

A log recording the sequence of events, with times and records of actions taken, must be maintained throughout the management process. All events will be investigated and analysed and used to improve the robustness of the organisation and its response to such incidents where possible.

Testing and Maintenance of the Plan

Key components of the plan will be tested on an annual basis, or sooner if significant changes to the Trust or its services are made. These tests will range from undertaking simple desk top

scenario-based exercises through to more complex simulations involving non-notice activation of the plan.

Records of all tests will be maintained, and the results of the tests routinely analysed and used to make improvements to the plan.

Preventative Strategies

It is vital education providers regularly review their existing defences and take the necessary steps to protect their networks. The Trust is following the DfE Cyber security standards for schools and colleges. In addition to this, there are several suggested measures that the Trust can implement to help improve IT security and mitigate the risk of a cyber-attack. Some of these will be fulfilled by the managed service provider, AIT:

- Regularly review IT Security, Online Security Policy and Data Protection Policy.
- Assess the school's current security measures against CyberEssentials requirements, such as firewall rules, malware protection, and role-based user access. Cyber Essentials is a government-backed baseline standard, which we would encourage all RPA members to strive towards achieving wherever possible.
- Ensure Multi-Factor Authentication (MFA) is in place: A method of confirming a user's identity by using a combination of two or more different factors.
- The MSP will implement a regular patching regime: Routinely install security and system updates and a regular patching regime to ensure any internet-facing device is not susceptible to an exploit. This includes Exchange servers, web servers, SQL servers, VPN devices and Firewall devices. Ensure that security patches are checked for and applied on a regular basis. Vulnerabilities within Microsoft Exchange Servers have been the root cause of many cyber-attacks in the last six months. It is highly recommended that on-premises exchange servers are reviewed and patched/updated as a high priority and moving to an Office 365 environment with MFA if possible.

- The MSP will enable and review Remote Device Protocols (RDP) access policies: The use of external RDP access to a device is not recommended and allows attackers to brute-force access to any device that is externally accessible. Mitigating measures are:
  - If external RDP connections are used, MFA should be used
  - Restricting access via the firewall to RDP enabled machines to allow only those who are allowed to connect
  - Enable an account lockout policy for failed attempts
  - The use of a VPN tunnel to access a network in the first instance, and then allowing users to subsequently use RDP or RDS to access a device afterwards is highly recommended
- Review NCSC advice regarding measures for IT teams to implement: Mitigating malware and ransomware attacks - NCSC.GOV.UK
- Provide awareness training for staff to recognise, report, and appropriately respond to security messages and/or suspicious activities.

Roles and Responsibilities

CEO

The CEO is responsible for the implementation and co-ordination of the Trust BCP, including:

- Immediately contacting the police if the disaster relates to the built environment or the ICT infrastructure to establish if the building can be re-occupied and/or service delivery reinstated.
- Co-ordination of status reports/communication for the benefit of all audiences (including staff, pupils, parents, LA, Academies Team at DFE, press).

• Maintaining the BCP in an up-to-date format by delegating responsibility to the Trust CFO.

Incident Management Team (IMT)
Led by the CEO, the IMT is made up of the Trust central team, including Estates Manager, CFO, , HR Manager, Trust Governance Manager, and the Director of School and People Development. Additional members of the team will be recruited to match the specific needs of the incident, for example the Exec team.

The IMT is responsible for acting under the direction of the CEO to restore normal conditions as soon as possible. If the central office is inaccessible the Estates Manager will indicate which of the schools to meet in; this will usually be Manor High School.

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

- Incident reported to the IMT Lead (CEO) or Deputy (appointed depending up on nature of incident)
- IMT Lead or Deputy takes decision as to whether the Business Continuity Plan needs to be invoked
- IMT Lead or Deputy decides whether Trust premises need to be evacuated – short or longer term
- Advise Risk Management Services and Insurance provider (Appendix 5)
- Advise Chair (and/or Vice Chair) of Trustees

The IMT Lead or Deputy has the authority to compel all central team and Exec members as relevant, to meet as soon as is reasonable as the IMT to discuss the incident, or the threat of an incident, which could force the BCP to be invoked.

Name	Role	Telephone (work)	Telephone (personal)	Email
Andy Wilson	CEO	0116 3033721 / 779		awilson@oaktrust.org
Paul Clarke	Estates Manager	0116 2714941/ 725		pclarke@oaktrust.org
Sarah Davis	CFO	0116 3033721 / 775		sdavis@oaktrust.org
Craig Brown	Director of School and People Development	0116 3033738 / 776		cbrown@oaktrust.org
Nicola Wall	HR Manager	0116 3033739 / 773		nwall@oaktrust.org
Danni Benyon-Payne	Governance Manager	0116 3033725 / 771		dbenyon-payne@oaktrust.org
If Trust wide incident – IMT will also include:				
Simon Greiff	MHS HT			sgreiff@manorhigh.leics.sch.uk

Hayley Brown	WGP HT			hbrown@woodlandgrange.leics.sch.uk
Grace Brown	BPS HT			gbrown@brookside.leics.sch.uk
Hayley Holmes	OIS HT			hholmes@overdale-inf.leicester.sch.uk
Matt Evans	OJS HT			m.evans@overdale-jun.leicester.sch.uk

Communication Plan

Liaison and Communication with the Emergency Services

If the emergency services are involved in the adverse event, then the CEO will appoint an individual from within its membership to act as a Liaison Officer.

Communicating with employees

At the earliest opportunity, all staff should be provided with information regards the adverse event, and instructions on further actions to be taken. IMT should arrange for a message to be sent to all staff information them of the adverse event and perceived impact on the operational effectiveness of the schools. IMT should also notify all Headteachers.

All staff that are affected but are off-site for any reason should also be informed of the adverse event without delay.

If the decision is taken to send staff home, or to wait at home while the situation is assessed, then arrangements should be made to contact them again within a specified time period to provide an update and fresh instructions.

Central team members should check their Kaizala team group.

Communicating with stakeholders

IMT will identify other persons and organisations who need to be informed of the event and will appoint a member of staff to keep these persons informed. This will include Trustees.

Communication with the Media

The IMT Lead will liaise with and answer any requests for information provided by the media.

In recognition of the importance to communicate a clear, concise and consistent message at a time when many of our stakeholders may be concerned with our operational effectiveness, all staff should refrain from answering any media enquiries, and instead, refer those enquires directly to the IMT Lead.

Procedure for Closing a school within the Oak Multi Academy Trust

Discussion to be held with CEO & Chair of Trustees to be informed.
Each school to invoke their BCP.

Business Recovery in the Event of a Loss of Buildings or site Space

General

Replacement of the buildings and facilities that have been damaged or made unavailable will be the responsibility of the Estates Manager. Temporary working facilities are the responsibility of the Trust. When possible, central staff will work from a location within Manor High school.

Insurance

CFO and Estates Manager will liaise with insurance underwriters.

Replacement Site Facilities

The size and scope of facilities required for the central team will vary according to circumstance. In the first instance contact should be made with the insurance underwriters. The location of the temporary accommodation will be determined by the Estates Manager based on the space required and circumstances at the time.

IT Systems Recovery

Loss of IT Systems

ICT systems are critical to the operation of the school and critical functions must be recovered within (48hrs) of any significant loss. Full recovery will take place within (10) days. There is a separate Major Incident Team for Trust wide IT issues (appendix 4).

Development of a 'ICT Disaster Recovery Plan' to recover the most critical service processes is the responsibility of the ICT Managed Service Provider (AIT) and contains the following elements:

• Identification of critical and secondary ICT needs.

• Arrangements for managing the complete loss of all or part of the system within the Trust and recovery of ICT systems for staff relocated into other areas, alternative sites, or working from home. This presumes that no equipment or material of any kind is available from the lost area.

• A strong data backup policy that provides a complete backup, on at least a daily basis.

• Robust procedures for the retention of premises related data such as surveys, records of remedial actions and statutory inspections.

• A detailed plan for restoring power, equipment, software, data, communications, and ancillary equipment to the identified locations within specified times.

Pandemic Threat / Mass Staff Unavailability

Loss of staff is considered a generic threat to operations. The spread of a virus capable of impacting on operational service delivery is now considered genuine and serious. In the event of mass staff illness or death, the CEO or, in their absence, the Chair of Trustees would refer to the Trustees and Headteachers.

Human Resource Recovery

Loss of people/ human resource is perhaps the most difficult type of loss to plan for as skills, knowledge and experience cannot be easily replaced, particularly in a short space of time.

Below are listed several key actions needed to reduce the risks associated with significant loss of human resource and mitigate against the impact of such an occurrence on the operational effectiveness of the Trust.

Planning actions prior to the adverse event

Ensure that critical jobs and functions have been identified within each area, and that adequate numbers of staff have the knowledge, skills and experience to perform these critical jobs and functions and thereby maintain the provision of the critical services.

Ensure that a few key staff have the skills, resources and relevant authorisations in order to work from remote locations. Mobile communication devices and access to relevant information to allow for service delivery are critical components of the resource requirements.

Actions to be taken / considered in the event of a significant human resource shortage

- Overtime payments or time off in lieu will be offered as appropriate.
- Temporary redeployment of staff across the Trust.
- Temporary reallocation of work activities within the central team.
- Temporary employment of agency staff / contractors and associate consultants.
- Prioritisation of work activities.
- Temporary suspension of non-essential work activities.

Infectious disease adverse events

For adverse events such as pandemic flu and other infectious diseases / viruses, the following measures may also be considered / implemented:

- Staff will be instructed to stay at home if they are ill or displaying certain symptoms to suggest they are becoming ill and are likely to spread the infection.
- Non-essential internal and external meetings / forums / training courses will be postponed, or where possible, held using remote electronic communication methods (web meetings, conference calls etc.).
- Flexible working arrangements will be introduced on a case-by-case basis to cater for a temporary change in individual staff's personal circumstances (e.g. provision of care to ill family member).

For business continuity

- Inventory of staff skills not utilised within their existing roles – to enable redeployment.

- Process mapping and documentation – to allow staff to undertake roles for which they are unfamiliar.
- Cross training of skills across a few individuals.
- Succession planning.
- Third party support backed by contractual agreements.
- Geographical/work pattern separation of individuals or groups can reduce the likelihood of losing all those capable undertaking a specific role.
- Where the incident lasts over a prolonged period then shift patterns should be considered and a handover process agreed.

Other Threats

The following "Other Threats" have been considered:

- Phone and ICT Communications Loss
- Finance Process Breakdown – payments to staff and suppliers fail
- Utilities / Energy Supply failure
- Evacuation due to Nearby Incident
- Bad Weather prolonged
- Terrorist Attack or Threat
- Biological or environmental hazard

Operational threat	**Steps to restore normal working**	**Action by whom**	**Comments / notes**
Phone and ICT Communications Loss	Contact AIT 0116 4828401	CFO	Keep CEO updated
Finance Process Breakdown – payments to staff and suppliers fail	CFO investigates issue Extent of situation is fully assessed Bank balances verified from online banking Staff and suppliers formally contacted with timescales / update	CFO	CEO, Chair of Finance & Resources Committee and Chair of Trustees kept updated

Utilities / Energy Supply failure	Providers called to ascertain issue Building may have to close Consider suitability of accessing a Generator	Estates Manager	Keep Chair of Trustees updated
Building Loss – partial or complete (Fire, Flood etc.)	Buildings services notified immediately Short-term – staff work remotely or at one of the schools, likely Manor High School Long term - rebuild / refurbish	Estates Manager	Buildings services will assign a designated Loss Adjuster
Building Denial leading to short term lack of access. Service Delivery Loss of General Nature –Trust unable to provide central team with building or ICT support	Relocate to the other schools within the MAT (likely Manor High School) or work from home	CEO and Estates Manager	
Evacuation due to nearby Incident	Evacuate immediately to designated assembly points at Manor High School inform CEO of any members of staff that are unaccounted for.	CEO	
Fire	Exit the building following Fire Evacuation plan Call Emergency services Call Buildings services regarding any damage Review what happened and capture any lessons learnt	CEO and Estates Manager	
Bad prolonged weather	Work remotely	CEO	

Terrorist Attack or Threat	Follow instructions from CEO either to: Evacuate immediately to designated assembly points at Manor High School Inform CEO of any members of staff that are unaccounted for OR Stay inside the building, well away from the windows and do not leave until instructed to do so by a member of IMT or the police/bomb squad	CEO	
Biological or Environmental hazard	Follow instructions from CEO either to: Evacuate immediately to designated assembly points at Manor High School Inform CEO of any members of staff that are unaccounted for OR Trigger IMT team & follow plan	CEO	

Appendix 1 - Checklist of Actions: Incident Management Team

Before the Event / Planning & Preparation

- Ensure all contact details are available, up-to-date, and accessible at all times.

During an adverse event

- Establish contact and lines of communication with other IMT members.
- Evaluate the impact of the adverse event and decide on the extent to which plan will be invoked.
- Direct actions of appropriate staff to implement the crisis management and recovery plans.
- Nominate a person to liaise with emergency services (as necessary).
- Nominate a person to liaise with the media (as necessary).
- Develop and agree on internal communications / messages (to affected staff)
- Nominate a person to act as focal point for internal communications in relation to the adverse event and provide regular news updates as required.
- Develop and agree on external communications / messages to external stakeholders (Trustees, members, suppliers etc.).
- Nominate a person to act as focal point for external communications in relation to the adverse event and provide regular news updates as required.
- Nominate a person to co-ordinate and arrange the transfer of telephone numbers.

Appendix 2: Incident Impact Assessment Form

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 3: Log Of Decisions, Actions, Contact and other Events

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

Appendix 4: IT Major incident team

School	Name	Email	Mobile number
Central Team - CEO	Andy Wilson	awilson@oaktrust.org	
Central Team - CFO	Sarah Davis	sdavis@oaktrust.org	
Central Team – Dir SPD	Craig Brown	cbrown@oaktrust.org	
BPS - Head	Grace Brown	gbrown@brookside.leics.sch.uk	
BPS - Office	Richard Skelton	rskelton@brookside.leics.sch.uk	
MHS - Head	Simon Greiff	sgreiff@manorhigh.leics.sch.uk	
MHS - Office	Alison Dawes	adawes@manorhigh.leics.sch.uk	
OIS - Head	Hayley Holmes	hholmes@overdale-inf.leicester.sch.uk	
OIS - Office	Jenny Robinson	jrobinson@overdale-inf.leicester.sch.uk	
OJS - Head	Matt Evans	m.evans@overdale-jun.leicester.sch.uk	
OJS - Office	Sarah Cooke	s.cooke@overdale-jun.leicester.sch.uk	
WGP - Head	Hayley Brown	head@woodlandgrange.leics.sch.uk	
WGP - Office	Netty Howard	ahoward@woodlandgrange.leics.sch.uk	

Appendix 5: Useful Telephone Numbers

Trust services	
AIT (ICT Managed Service Provider)	0116 4828401
LAIS (Insurance Provider)	0116 305 6516
Leicestershire Food Services (Catering)	0116 305 5770
Flint Bishop (HR)	01332 226 155
Trust schools	
Brookside Primary school	0116 271 3680
Manor High School	0116 271 4941
Overdale Infant School	0116 288 2724
Overdale Junior School	0116 288 3736
Woodland Grange Primary School	0116 272 0401
Leicester City Council	
Risk Management Services	0116 454 1635
Learning Services	0116 454 1927
Transport services	0116 252 7802
City Hall Security	0116 373 7770
Health and Safety Team	0116 454 4307/4311/4315
Emergency Management Unit (LCC)	0116 373 6613 or 0116 454 3621 / 0116 454 3622
Leicestershire County Council	
Children And Young People Services	0116 2323232
Children and Family Wellbeing	0116 3058727
Transport services	0116 3058777
Educational Visits H&S	0116 3055515
Emergency Planning H&S	0116 3055515
Educational Psychology Service	0116 3055100
Health and Safety Team	0116 3055515
Major Incident Team	07786 198283
Media	
BBC Radio Leicester	0116 2561355
Radio Leicester	0116 2516688
Other services	
Police, Fire and Ambulance	999 (24 hour)
Police	101 (24-hour, non-emergency number)
Department for Education	0370 000 2288 (office hours, general enquiries)
Foreign and Commonwealth	0207 008 1500 (24-hour, consular assistance)
Environment Agency	0845 988 1188 (24 hour, floodline)
Teacher Support Network	08000 562 561 (24 hour)

Appendix 6: Action Plan

1. Actions in the event of an incident

If you suspect you have been the victim of a ransomware or other cyber incident, you should take the following steps immediately:

- Enact your Cyber Recovery Plan
- Contact the 24/7/365 RPA Cyber Emergency Assistance:
    - By telephone: **0800 368 6378** or by email: **RPAresponse@CyberClan.com**
    - You will receive a guaranteed response within 15 minutes
    - Incident information will be recorded, advice will be provided and any critical ongoing incidents will be contained where possible
    - Subject to the claim being determined as valid, an expert Incident Response team will be deployed to rapidly respond to the incident, providing Incident Response services including: forensic investigation services and support in bringing IT operations securely back up and running.
- Inform the National Cyber Security Centre (NCSC) - https://report.ncsc.gov.uk
- Contact your local police via Action Fraud Action Fraud website or call **0300 123 2040**
- If you are a part of a Local Authority (LA), they should be contacted
- Contact your Data Protection Officer
- Consider whether reporting to the ICO is necessary report at www.ico.org.uk **0303 123 1112**
- Contact the Sector Security Enquiries Team at the Department for Education by emailing: sector.securityenquiries@education.gov.uk

Please be aware that speed is of critical importance during a cyber incident to help protect and recover any systems that may have been affected and help prevent further spread.

2. Cyber Recovery Plan

1. Verify the initial incident report as genuine and record on the Incident Recovery Event Recording Form at Appendix C.
2. Assess and document the scope of the incident using the Incident Impact Assessment at Appendix A to identify which key functions are operational / which are affected.
3. In the event of a suspected cyber-attack, IT staff should isolate devices from the network.

4. In order to assist data recovery, if damage to a computer or back up material is suspected, staff **should not:**
    - Turn off electrical power to any computer.
    - Try to run any hard drive, back up disc or tape to try to retrieve data.
    - Tamper with or move damaged computers, discs or tapes.
5. Contact RPA Emergency Assistance Helpline.
6. Start the Actions Log to record recovery steps and monitor progress.
7. Convene the Cyber Recovery Team (CRT).
8. Liaise with IT staff to estimate the recovery time and likely impact.
9. Make a decision as to the safety of the school remaining open.
    - *This will be in liaison with relevant Local Authority Support Services / Trust*
10. Identify legal obligations and any required statutory reporting e.g., criminal acts / reports to the Information Commissioner's Office in the event of a data breach.
    - *This may involve the school's Data Protection Officer and the police*
11. Execute the communication strategy which should include a media / press release if applicable.
    - *Communications with staff, governors and parents / pupils should follow in that order, prior to the media release.*
12. Make adjustments to recovery timescales as time progresses and keep stakeholders informed.
13. Upon completion of the process, evaluate the effectiveness of the response using the Post Incident Evaluation at Appendix D and review the Cyber Recovery Plan accordingly.
14. Educate employees on avoiding similar incidents / implement lessons learned.

Ensure this plan is kept up-to-date with new suppliers, new contact details, and changes to policy.