Northern College

1. Overview

Policy Title	**Business Continuity**
Who does the policy apply to?	All employees and anyone acting for, or on behalf of the College including governors, other volunteers, temporary workers, consultants and contractors.
Aims	To set out the College's approach to business continuity and outline procedures in the event of a major incident.
To be read in conjunction with	Risk Management Policy Risk Register Duty Manager Procedures
Further advice may be sought from	Deputy Principal / Chief Finance Officer
Review arrangements	This policy will be reviewed every three years to ensure its continuing relevance and effectiveness. The College may review the policy prior to this date should operational and/or legislative/guidance matters require it. Further details regarding revisions and review cycle can be found at para 9.

2. Introduction

2.1. The Business Continuity Policy (the policy) forms part of the College's internal control and corporate governance arrangements.

2.2. The policy is issued as part of the College's overall system of risk management and control, as set out in the Risk Management Policy and Financial Regulations. The College's risk management control processes involve the identification, evaluation and management of significant risks faced by the College in achieving its goals, which are under regular review by the Executive Leadership Team and the Corporation and its committees.

2.3. A major incident plan (the plan), attached at appendix B, is issued to support particular members of staff in the event of a situation which requires a response to prevent or minimise the impact on College business.

2.4. A Major Incident Management Team (MIMT), membership of which is outlined in Appendix A, will deal with any incident which requires the plan to be put into place. The team may include any additional members as required in order to effectively deal with a particular incident.

2.5. The College's Risk Management and Business Continuity Group will oversee ongoing review and development of the College's business continuity arrangements.

2.6. Staff are asked to ensure that they read and understand the contents of this policy and to ensure that they remain aware of its contents in order to act appropriately should an issue affect the College.

3. Aims and Objectives

3.1. The main aims of the policy are to:

3.1.1. create an awareness of the need for business continuity planning and development;
3.1.2. provide a planning framework for responding to major incidents;
3.1.3. identify major areas of risk for business continuity planning;

3.1.4. outline the responsibilities of individuals and groups;
3.1.5. identify staff members who should be members of the Major Incident Management Team;
3.1.6. outline training and testing needs.

3.2. The two main aims of the plan are:

3.2.1. to prevent or limit loss of life or injury, and limit or minimise damage to assets and/or buildings (emergency recovery);
3.2.2. to bring the College back into full operation with minimal disruption to students and staff (business recovery).

3.3. The main aims will be addressed by coordinating the response of all departments and staff in the event of a major incident to ensure that business critical functions are reinstated as soon as possible and all services are restored as quickly as practical.

4. Areas of Risk

4.1. The major areas of risk for business continuity for the College have been identified as:

4.1.1. closure or partial closure of the campus for example as a result of fire, loss of services, flood, adverse weather conditions, bomb threat or other incident;
4.1.2. loss of life and/ or major injury sustained on or off site;
4.1.3. major infection/ illness forcing closure or partial closure of the campus;
4.1.4. major loss of IT capacity due to theft, hacking, virus, equipment failure or damage.

5. Employing the Plan

5.1. The plan will come into effect when a major incident is taking place or has taken place.

5.2. There may be incidents where an immediate response is required to protect life and property, for example a gas leak is detected or an immediate bomb threat is received. In this case it may not be practical to convene an MIMT meeting and an immediate response should be made.

5.3. Immediate action should be taken by the person discovering the risk. This may involve:

5.3.1. contacting emergency services;
5.3.2. notifying a line manager or assistant principal;
5.3.3. receiving and conveying instructions from either party.

5.4. The MIMT would be called together to consider its response to the incident when practical.

5.5. The plan includes general guidance, however it is accepted that individual instances may well be unique, and responses and approaches may vary accordingly.

6. Responsibilities

6.1. The **Board of Governors** is responsible for:

6.1.1. safeguarding the assets of the College and overseeing the procedures in place for managing business risks;
6.1.2. setting the tone and influencing the culture of risk management within the College, including the level of acceptable risk on a case-by-case basis;

6.1.3. periodically approving the policy on the advice and guidance of the Audit Committee.

6.2. The **Audit Committee** will be responsible for:

6.2.1. advising the Board of Governors on the system of internal controls, risk management and governance - as business continuity impacts on all of these areas, the Audit Committee will be required to approve and recommend the policy to the Board of Governors;

6.2.2. periodically reviewing the policy;

6.2.3. providing advice to the Board of Governors on the effectiveness of the internal control system;

6.2.4. receiving a detailed report or update relating to any business continuity issues.

6.3. The **Executive Leadership Team** is responsible for:

6.3.1. commissioning the policy and recommending it to the Corporation for approval;

6.3.2. any decision on the closure, or part closure of the campus;

6.3.3. overseeing the College's business continuity arrangements.

6.4. The **Deputy Principal / Chief Finance Officer** is responsible for:

6.4.1. the development and maintenance of the policy and the plan;

6.4.2. the upkeep and communication of an emergency closure plan, which deals with the communication process for closing the College campus;

6.4.3. testing and rehearsing the plan with the support of the Risk and Business Continuity Group;

6.4.4. training of members of the Major Incident Management Team and Risk and Business Continuity Group.

6.4.5 In the event of a major incident, a post disruption review is undertaken to ensure that all lessons learnt are captured.

6.5. The **Major Incident Management Team Chair** is responsible for:

6.5.1. convening and managing the MIMT during an incident;

6.5.2. involving other relevant personnel as needed;

6.5.3. declaring an incident over and allowing the plan to be closed down.

6.6. The **Major Incident Management Team** is responsible for

6.6.1. the implementation of the plan during an incident - all members should hold a copy of the plan at work and at home;

6.6.2. feeding back to the Risk and Business Continuity Group any issues or recommendations arising from the implementation of the Plan.

6.7. The **Risk and Business Continuity Group** is responsible for:

6.7.1. the identification and prioritisation of critical business processes within the College, and the business impact assessment of the loss or impairment of these processes;

6.7.2. devising appropriate methods and processes for the recovery of the critical business processes;

6.7.3. the review, development and update of the plan, and considering developments in the field of business continuity internally and externally.

6.8. Members of the **College Leadership Team** are responsible for:

6.8.1. raising awareness of business continuity in their departments and distributing relevant information and materials to their teams;

6.8.2. having their own recovery plan and/or procedures to aid emergency and business recovery in a given incident. This plan should focus on the departments own functions including student welfare and support in curriculum areas. In incidents which are unlikely to affect the College as a whole, these departmental plans may be initiated by the departmental head, who should inform the Executive Leadership Team of their decision.

6.9. **All members of staff** are responsible for:

6.9.1. ensuring that they operate at College in such a way as to minimise the risk of a business interruption incident occurring;

6.9.2. raising with their line manager any real or perceived risk which may impact on the business continuity of the College.

7. Training

7.1. It is essential that all key staff are updated with:

7.1.1. changes to the policy and plan;

7.1.2. changes to the members and details of the various groups;

7.1.3. significant changes to critical business functions and processes;

7.1.4. links with other policies.

7.2. Training for the various groups should be carried out regularly and at least once per year. Training may take the form of updating or rehearsal.

8. Testing

8.1. Testing of the plan should be carried out annually by the Deputy Principal / Chief Finance Officer. The testing should include:

8.1.1. checks of staff members in post and their contact details;

8.1.2. check that all members of the distribution list (see the appendices) retain copies of the plan at work and at home;

8.1.3. check that there are no additional or redundant business processes.

8.2. Rehearsal of the plan should be carried out annually by the Deputy Principal / Chief Finance Officer supported by the ELT and the Risk and Business Continuity Group. The rehearsal should:

8.2.1. involve a walk-through desktop exercise based on varying scenarios reflecting the key areas of risk;

8.2.2. generate feedback to help further develop and refine the plan (and policy) in the future.

9. Policy sign off and ownership details

Document Name:	Business Continuity Policy
Version Number:	3.0
Effective from:	March 2024
Next scheduled review date:	March 2027
Policy owner:	Deputy Principal / Chief Finance Officer
Approved by:	Board of Governors

10. Revision history

Version No	Effective date	Revision description/summary of changes	Author
2.0	11 March 2021	Complete re-write.	AP – FBS (Joy Whistlecraft)
3.0	25 March 2024	Update of roles and minor changes	DP/CFO (Sue Saunders)

Appendix A
Incident Management Team

Job Title	Area of Responsibility
Deputy Principal / Chief Finance Officer (chair)	Finance/IT/ MIS/ business services
Principal	Chair/External stakeholders External communications (supported by Marketing Manager)
Assistant Principal - Student Experience	Student experience/Safeguarding
Director of Curriculum & Quality	Curriculum matters/inspection / quality
Head of HR	Staff/training. Internal Communications
Head of Finance	Finance/Payroll
Head of MIS & ICT	MIS / Exams /ICT / Cyber Security
Curriculum Manager – Essential Skills	Curriculum
Curriculum Manager – Society, Health and Development	Curriculum
Head of Estates	Insurance, Estates and H&S (inc catering, security and cleaning)
Head of Student Support Services	Student services/Additional Learning Support/Library/frontline
Clerk to the Governors/Data Protection Officer	Liaison/communication with governors/data protection.

Appendix B Major Incident Management Plan

1. The purpose of this major incident management plan is to:
   1.1. provide a process for evaluating whether a major incident is occurring;
   1.2. provide a framework for maintaining the College's services in the event of an incident causing serious disruption;
   1.3. ensure the welfare and security of College students and staff;
   1.4. secure and protect the College environment.

2. The objectives of the plan are to:
   2.1. respond effectively to an incident;
   2.2. minimise the risk of disruption to College services;
   2.3. maintain the College's services;
   2.4. communicate with College staff, students and stakeholders during an incident.

3. The plan will be activated and carried through by the Major Incident Management Team (MIMT) as set out in the Business Continuity Policy.

4. <u>Assessment and Escalation Procedure</u>

4.1. On receiving notification of a potential major incident the Deputy Principal / Chief Finance Officer, or in their absence another member of the Executive Leadership Team, will assess the situation using the attached tables 1 and 2.

4.2. Where:

4.2.1. a level 4 incident is deemed to be occurring or imminent the MIMT will be convened;

4.2.2. a level 3 incident is deemed to be occurring or imminent the MIMT will meet to consider issues and monitor the situation to assess potential activation of the plan should the situation escalate;

4.2.3. a level 2 incident is deemed to be occurring or imminent the MIMT will be placed on standby for potential activation of the plan and the situation will continue to be managed through normal processes;

4.2.4. a level 1 incident is deemed to be occurring or imminent it will be managed through normal processes.

5. Procedure for the Major Incident Management Team

5.1. The varying nature of incidents means that bespoke management of any situation will be required, however the following checklist should be considered:

Set up	○ MIMT room/meeting/communication/ICT requirements ○ Establish operational base requirements in event of complete campus closure ○ MIMT record keeping requirements ○ Brief MIMT
Evaluation	○ establish information or knowledge gaps ○ record factual information

	○ evaluate degree of threat, current and potential future impacts, potential for escalation or spread ○ define recovery objectives and operational constraints ○ agree the College's priorities at this time ○ agree MIMT objectives ○ ensure the budget, financial constraints are identified and accounted for

	Aspects	**Example areas to consider**
	health and safety	• casualties/injuries and response required • first aid/emergency services • evacuation arrangements • cordons/physical safety measures required • any Safeguarding matters
	students	• impact on curriculum delivery • impact on accommodation/food/safety • impact on other support/operational needs
	staff	• impact on staff working arrangements/operational needs • additional/changed staffing needs • employment contracts and implications of temporary or permanent changes to staff terms and conditions
	communications	• communication plan – messages, spokesperson(s), audiences, timetable, communication channels • monitoring incoming information and trends and developments • potential media interest and response plan • next of kin notifications • staff and student briefings
	support	• counselling needs or other support services • general guidance/support/wellbeing requirements
	stakeholder interests	• governors – briefing/approvals/meetings • funders • partners • local authorities • emergency services • contractors/service providers

	ICT	• equipment loss (servers, applications, databases, voice and data communications, client PCs) • ICT service recovery/hardware requirements/recovery timetable • impact of recovery constraints • manual workarounds • provision of remote working
	data protection	• permanent/temporary loss of data and potential impact • notification requirements e.g. data subjects/ICO • data security and recovery
	buildings and property	• inaccessible areas • hazard areas • structural condition • safe level of occupation
		• electricity supply • gas supply • water supply • air conditioning • fire detection • initial and longer term recovery works required and costs/timetable • alternative site(s) and redeployment activities • liaison with insurers and loss adjusters • liaison with National Trust
	security	• maintenance of site security arrangements
recovery/reinstatement	○ recovery objectives, timetable and plan ○ risks to recovery ○ resource needs	
stand-down	○ write up incident records ○ post–emergency briefing and thank yous ○ liaison with stakeholders to provide reassurance/visibility ○ review status of business continuity related actions, identifying assistance / support required from MIMT members ○ arrangements to ensure any resources that may be needed to support a future emergency response are replenished ○ full review of emergency and response to ensure that improvement actions are identified and implemented	

Table 1 – Incident Evaluation

IMPACT ASSESSMENT TABLE		
Incident level	Definition	One or more of the following apply
1	Minor incident	The incident is not serious or widespread and is unlikely to affect business operations or College reputation to a significant degree. The incident can be dealt with through normal processes.
Response/action: Incident is managed through normal processes		
Incident level	Definition	One or more of the following apply
2	Incident causing minor disruption and/or reputational threat	Incident expected to be fully resolved within four hours. Access to systems is denied but expected to be resolved within four hours. Potential threat to College reputation low.
Response/action: MIMT placed on standby for potential activation of plan		
Incident level	Definition	One or more of the following apply
3	Significant disruption and/or reputational threat	Disruption is likely to last for more than one working day. Access to parts of the campus denied for more than 24 hours. Access to systems denied and incident expected to last more than one working day. A significant threat to the College's reputation has been identified
Response/action: MIMT meet to consider next steps and potential activation of plan should the situation escalate		
Incident level	Definition	One or more of the following apply
4	Major disruption and/or reputational threat	Destructive loss to the campus. Major wide scale incident in local area affecting the College. Significant disruption to business activities. Significant event with immediate potential for serious reputational damage
Response/action: Immediate activation of plan, full MIMT convened		

Table 2 – Incident Evaluation

Incident Categorisation				
Incident description	**Level 1** Incident may be managed by College staff	**Level 2** MIMT placed on standby	**Level 3** MIMT consider situation	**Level 4** Mandatory meeting of the MIT
Loss or failure of minor systems	✓			
Minor loss of assets	✓			
Sudden reduction in available staff		✓		
Issue affecting reputation of college locally		✓		
Loss of Utilities: gas, electricity or water			✓	
Restricted access to site			✓	
Loss of communications			✓	
Loss or failure of mission critical systems			✓	
Situation requiring lockdown of campus				✓
Serious damage to building				✓
Significant loss of or serious damage to assets				✓
Serious injury/fatality				✓
Issue affecting reputation of college regionally or nationally				✓
Loss of life				✓
Loss of one or more buildings				✓