University of Manchester Library – Business Continuity Plan

Introduction

The University of Manchester Library provides essential learning, research and workspace for hundreds of staff and thousands of students, as well as holding critical teaching and research collections. The loss of some or all of the facilities could have a serious impact on students, staff and researchers, and consequently on the reputation and finances of the University.

The University has an agreed methodology for incident management and business continuity, and this plan has been developed in partnership with Risk and Compliance to ensure it is aligned with, and integrated with, wider University plans.

Plan Summary

Plan Owner	University Librarian and Director of The John Rylands Library
Deputy Plan Owner	Library Leadership Team Incident Manager Lead
Aims	The aims of this plan are to identify and describe the steps to be taken in response to incidents which disrupt business at any Library site, so that immediate issues are well-managed, and services restored as quickly as possible.
Objectives	• To ensure that the Library is integrated with other University business continuity planning and in particular with the University's Major Incident Response Plan. • To provide an effective response to the loss of service as a result of a serious incident (e.g. accidental damage, power loss, staff shortages, cyber-attack) • To ensure rapid and appropriate restoration of services, in alternative locations if required, for library staff and customers. • To support effective communication throughout the incident response, interim management and service recovery phases.
Scope	This plan relates specifically to the loss of resources, services, staff and building space managed by the Library. This document follows agreed university guidelines for business continuity and is integrated with the University Emergency Management Plan Emergency planning | Compliance and Risk | StaffNet | The University of Manchester This plan is top-level and references other plans and procedures where necessary to avoid duplication, ensure consistency of approach and mitigate extended periods of disruption as a result of inefficiency or confusion. This plan is designed to respond to significant incidents. While it is difficult to define these precisely, they would likely be of a scale sufficient to result in a site closure or suspension of a service.
Version Control	v1.15 March 2026

The immediate response to an incident will depend on whether it has been defined as a University Major Incident. If it has, the Library will be brought into a wider University response as required (Category One). Otherwise, the steps listed in Category Two will apply.

Action Plan

Decision made at University Level to invoke the Major incident Response Plan (Category One)

Action	Responsible Person	Duration (cumulative)	Notes
A Library Executive Team (LET) member is notified of the incident by the President, Registrar or other member of staff with authority to invoke the Major Incident Response Plan.	President Registrar Director of Risk and Compliance University Emergency Incident Manager (EIM)		University Major incident policy [Director or nominee joins Silver command]
LET member appoints an overall Library Incident Manager (Library IM).	LET member	15 mins	Appointment will depend on the nature and severity of the incident, its time and location, and the availability of appropriate and trained staff. If the incident is a cyber-attack, the library response procedure is documented in the Library Cyber Run Book.

Any Other Serious Incident (Category Two)

Phase One: Assessment/Incident response

An incident is reported to Library management (by a member of Library staff, or via Security, the EIM or a customer).	Alerted Manager		All managers will have been trained to identify whether incidents should invoke this plan and will take appropriate action.
Trigger alarm and evacuation procedures if the nature of the incident requires it.	Alerted Manager	2 mins	Hand over control to a Lead Fire Marshal if appropriate.
If the incident is sufficiently serious, contact University Security on 0161 306 9966.	Alerted Manager	2 mins	Security telephone number is on the back of staff ID cards.
If the incident is defined as a University Major Incident, alert the University Librarian and Director of The John Rylands Library (University Librarian) or other available member of LET, who should await further instructions.	Alerted Manager/LET member	5 mins	Refer to Category One.
If the incident is not a University Major Incident, but is significant, alert the University Librarian or other available member of LET, who will appoint a Library Incident manager (Library IM), who will take responsibility for further steps.	Manager	5 mins	
Establish the extent of any health and safety issues and confirm that these are being managed.	Library IM	10 mins	
Alert the Head of Engagement and/or the Engagement Managers and instigate the Library incidents communication plan.	Library IM / Head of Engagement / Engagement Manager	10 mins	
Assess impact on Library services and administration to determine any need to close sites, and/or relocate services and staff, and	Library IM	20 mins	

establish likely duration of disruption.			
If there is damage, or risk of damage, to collections, contact the Collection Care Manager or University Librarian who will determine whether to invoke the Collections Disaster Plan.	Library IM/Collection Care Manager / University Librarian	20 mins	
If the incident affects IT infrastructure due to loss of power, network, or access to hardware, alert the Director of Artificial Intelligence and Ideas Adoption or other member of the AIIA DMT. Library system continuity is supported by the Digital business continuity plan. If the incident is a suspected cyber-attack, contact ITS immediately.	Library IM/ Director of Artificial Intelligence and Ideas Adoption	20 mins	If IT incidents occur elsewhere, IT Services will inform the Library's digital team who will assess the impact on Library services (and in the case of some critical business systems, users of that system) who will then instigate the agreed communications plan.

Phase Two – Recovery and Interim Service

Action	Responsible Person	Duration	Notes
Liaise with University Security (or the EIM via University Security) if as appropriate, e.g. on the condition of an affected site and duration of closure.	Library IM	I hour	
If appropriate, liaise hourly with the University Security University Security (or the EIM via University Security) on state of building and access.	Library IM		

Assess the need for temporary office space and/or relocation to other sites.	Library IM	2 hours	If there is a need to relocate staff, it is likely that the University will define it as a major incident. Temporary office space can be made available in such cases.
Liaise with Risk and Compliance and Estates if temporary office space is required.	Library IM	2 hours	
Determine service needs such as the provision of additional study space, access to collections and use of alternative facilities.	Library IM	2 hours	This will depend on the expected duration of loss of facilities, and tolerance of disruption. Time of year will be a factor as it will impact demand for services. In the case of the loss of digital services available mitigations are documented in the Digital Business Continuity Plan.
Draft communications for staff and customers informing them of the incident, and the interim arrangements and their anticipated duration.	Library IM, plus Engagement Manager or delegate	3 hours	
Sign off the communications plan and release.	Engagement Manager and either University Librarian or available member of LET	1 hour	
Establish service levels for temporary study spaces, and hand over management arrangements to appropriate Library Experience Team Manager.	Library IM	4 hours	Agree temporary office spaces and equipment and arrange handover.

Phase Three – Ongoing management

Establish an incident management/business continuity task group for ongoing management of the incident and business continuity/recovery.

Roles to be considered for inclusion include

- Engagement
- Health & Safety
- Owners of affected Business Continuity Plans
- Library Experience Team
- Rylands Services
- Digital Services
- Library Spaces Coordinator

Typical actions include

- Ensure regular communications continue as instructed in the communications plan.
- Ensure that health and safety requirements continue to be met at alternative location.
- Estimate period of temporary working arrangements.
- Coordinate the initiation of Business Continuity Plans.

Key Services

The services listed below have been prioritised after consultation with managers across the Library, using a methodology provided by Risk and Compliance. The context of any incident will be a major determining factor in deciding on priorities and responses, so this list is simply a guide, which should not override management decisions on the ground in the event of an incident. Service priorities will be determined by, for example, the nature of an incident (e.g. power loss or building closure), its severity (which affects the duration of disruption), the time of year (e.g. exam periods), and the strategic impact.

	Name of Service	Manager	Notes
1	Access to digital library and extended digital collections	Ciaran Talbot	
2	Security of buildings and collections	Sandra Bracegirdle Heather Cole	
3	Digital experience	Ciaran Talbot	
4	Alma/Library Search/e-resources/reading list system	Amin Hussain	ITS are aware that this is high priority
5	eThesis service	Ian Gifford	
6	Study space	Katy Woolfenden	
7	Provision of printed materials where access is prevented.	Sandra Bracegirdle	Risk of flooding especially
8	Self-service loans/returns	Natalie Patton	

9	Access to IT for students	Martin O'Dwyer	
10	Access to physical Collections	Sandra Bracegirdle	Risk of flooding especially
11	Enquiry services	Natalie Patton	
12	REF open access curation	Scott Taylor	
13	Staff digital workspace and technical	Amin Hussain	
14	APC payments	Lucy May	
15	Conservation/preservation of existing collections	Elizabeth Carr	
16	Collection management purchasing & supply	Rachel Schulkins	
17	Library finances	Sandra Bracegirdle	
18	Library administration (including Data Protection)	Peter Wadsworth	