

**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

<b>Plan Owner</b>	<b>John Rylands University Librarian and Director of the University of Manchester Library</b>
<b>Deputy Plan Owner</b>	Library Incident Managers lead
<b>Aims</b>	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.
<b>Objectives</b>	<ul style="list-style-type: none"> <li>• To ensure that the Library is integrated with other University business continuity planning and in particular with the University's Major Incident Response Plan.</li> <li>• 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)</li> <li>• To ensure rapid and appropriate restoration of services, in alternative locations if required, for library staff and customers.</li> <li>• To support effective communication throughout the incident response, interim management and service recovery phases.</li> </ul>

**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 of Manchester Major Incident Response Plan (Version 2.0 revised 2019).

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**

v1.14 March 2022

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	Notes
<b>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.</b>	President Registrar Director of Risk and Compliance University Emergency Incident Manager (EIM)		University Major incident policy [Director or nominee joins Silver command]
<b>LET member appoints an overall Library Incident Manager (Library IM).</b>	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**

<p>An incident is reported to Library management (by a member of Library staff, or via Security, the EIM or a customer).</p>	<p>Alerted Manager</p>		<p>All managers will have been trained to identify whether incidents should invoke this plan and will take appropriate action.</p>
<p>Trigger alarm and evacuation procedures if the nature of the incident requires it.</p>	<p>Alerted Manager</p>	<p>5 mins</p>	<p>Hand over control to a Lead Fire Marshal if appropriate.</p>
<p>If the incident is sufficiently serious, contact University Security on 0161 306 9966</p>	<p>Alerted Manager</p>	<p>5 mins</p>	<p>Security telephone number is on the back of staff ID cards.</p>
<p>If the incident is defined as a University Major Incident, alert the John Rylands University Librarian and Director of the University of Manchester Library (University Librarian) or other available member of LET, who should await further instructions.</p>	<p>Alerted Manager/LET member</p>	<p>5 mins</p>	<p>Refer to Category One.</p>
<p>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</p>	<p>Manager</p>	<p>5 mins</p>	

<b>Establish the extent of any health and safety issues and confirm that these are being managed.</b>	Library IM	10 mins	
<b>Alert the Communications and Engagement Manager and instigate the Library incidents communication plan</b>	Library IM / Communications and Engagement Manager	10 mins	
<b>Assess impact on Library services and administration to determine any need to close sites, and/or relocate services and staff, and establish likely duration of disruption.</b>	Library IM	20 mins	
<b>If there is damage, or risk of damage, to collections, contact the Collection Care Manager or Associate Director: Collection Strategies Curatorial Practices who will determine whether to invoke the Collections Disaster Plan.</b>	Library IM/Collection Care Manager/Head of Collection Strategies	20 mins	
<b>If the incident affects IT infrastructure due to loss of power, network, or access to hardware, alert the Associate Director: Research and Digital Horizons or Library Systems Support Manager. Library system continuity is supported by the Digital business continuity plan. If the incident is a suspected cyber-attack, contact ITS immediately.</b>	Library IM/AD RDH/Library Systems Support Manager	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**

<b>Action</b>	<b>Responsible Person</b>	<b>Duration</b>	<b>Notes</b>
<b>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.</b>	Library IM	1 hour	
<b>If appropriate, liaise hourly with the University Security University Security (or the EIM via University Security) on state of building and access.</b>	Library IM		
<b>Assess the need for temporary office space and/or relocation to other sites.</b>	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.
<b>Liaise with Risk and Compliance and Estates if temporary office space is required.</b>	Library IM	2 hours	
<b>Determine service needs such as the provision of additional study space, access to collections and use of alternative facilities.</b>	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.
<b>Draft communications for staff and customers informing them of the incident, and the interim arrangements and their anticipated duration.</b>	Library IM, plus Communications and Engagement Manager or delegate	3 hours	



<b>Sign off the communications plan and release.</b>	Communications and Engagement Manager and either University Librarian or available member of LET	1 hour	
<b>Establish service levels for temporary study spaces, and hand over management arrangements to appropriate Customer Services Manager.</b>	Library IM	4 hours	Agree temporary office spaces and equipment and arrange handover.

**Phase Three – Ongoing management**

<b>Action</b>	<b>Responsible Person</b>	<b>Duration</b>	<b>Notes</b>
<b>Ensure regular communications continue as instructed in the communications plan.</b>	Communications and Engagement Manager or delegate		
<b>Ensure that health and safety requirements continue to be met at alternative location.</b>	Library IM	5 hours	
<b>Estimate period of temporary working arrangements.</b>	Library IM		
<b>Arrange to hand over management of interim services and accommodation to appropriate Library managers.</b>	Library IM	6 hours	

### 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.

The list has been amended whilst we are working remotely away from campus to reflect the new priorities – newly added services are in red; physical services that aren't currently relevant are struck out.

	<b>Name of Service</b>	<b>Manager</b>	<b>Notes</b>
1	Access to digital library and extended digital collections	Lorraine Beard	
2	Security of buildings and collections	Sandra Bracegirdle Jane Gallagher	
3	Digital experience	Ciaran Talbot	
4	Alma/Library Search/e-resources/reading list system	Ciaran Talbot	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	Debbie Allan	

10

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