

BUSINESS CONTINUITY POLICY

Policies superseded by this version

This document replaces version 1.0 of the Business Continuity Policy (March 2023), with effect from 09 June 2026.

Summary of changes to previous version

Version History

Version	Date	Summary of Changes	Author
1.0	March 2023	Initial approved policy (City, University of London) This policy (version 1.0) was approved by SLT in December 2022 and by the Audit and Risk Committee (ARC) in March 2023. This document will replace version 1.0 with effect from the date of approval.	
2.0	2026	Updated following post-merger review: <ul style="list-style-type: none"> • Merger of City, University of London with St George's, University of London (August 2024), creating City St George's, University of London • Enhanced focus on cross-site dependencies and dual-campus operations across Clerkenwell and Tooting • Addition of Legal and Regulatory Responsibilities section (incorporating Martyn's Law (Terrorism (Protection of Premises) Act 2025)), reflecting governance decisions confirmed at the University Security Governance Meeting (May 2026); detailed compliance content sits within a dedicated Martyn's Law policy and procedures 	Risk & BCM Manager

Table of Contents

1. Introduction.....	3
2. Freedom of Speech and Academic Freedom	3
3. Equality, Diversity and Inclusion.....	3
4. Definitions.....	3
5. Policy.....	4
6. Procedure	6

7. Advice and Guidance.....9

8. Legal and Regulatory Responsibilities 12

9. Failure to Comply9

10. Review 10

Appendix A – Key Performance Targets 13

Appendix B – Supporting Documentation 13

1. Introduction

This policy sets out the principles and framework for Business Continuity Management at City St George's, University of London. It meets requirements of ISO 22301:2019, the Office for Students (OfS), and good practice in the higher education sector.

The merger of City, University of London with St George's, University of London in August 2024 has created a multi-campus institution operating across Clerkenwell, Moorgate and Tooting, with shared services, cross-site IT infrastructure, and significant operational dependencies on NHS-owned estate. Recent major incidents including the Cyber incident (March 2026) and Hunter Wing flooding (July 2025) have demonstrated the critical importance of well-tested continuity arrangements.

2. Freedom of Speech and Academic Freedom

- 2.1. City St George's, University of London, regards freedom of speech and academic freedom to be fundamental to delivering its mission as the University of business, practice and the professions. Its values in this respect are set out in a code of practice on freedom of speech and academic freedom, which explains how the University will uphold, secure, and promote freedom of speech within the law: <https://www.citystgeorges.ac.uk/about/governance/policies/code-of-practice-on-freedom-of-speech>.
- 2.2. Nothing in this policy should be interpreted in any way that would be inconsistent with the code of practice and – in the event of any inconsistency – the provisions of the code will prevail.
- 2.3. The Office for Students ("OfS") operates a free speech complaints scheme. Under that scheme, the OfS can review complaints about free speech from non-student members, staff, applicants for academic posts and (actual or invited) visiting speakers. The scheme is free to use. Information about the complaints that the OfS can review is available on its website at: www.officeforstudents.org.uk/for-providers/freedom-of-speech/free-speech-complaints. Student complaints about freedom of speech issues are handled by the Office of the Independent Adjudicator for Higher Education ("OIA"). Information about how the OIA handles such complaints can be found on its website (<https://www.oiahe.org.uk/resources-and-publications/latest-news-and-updates/oia-highlights-role-in-student-free-speech-complaints/>).

3. Equality, Diversity and Inclusion

- 3.1. The University is committed to promoting equality, diversity and inclusion in all its activities, processes, and culture for our whole community, including staff, students and visitors.
- 3.2. The University will meet its obligations under the Equality Act 2010 in all its policies and will seek to eliminate discrimination based on age, caring responsibilities, disability, gender identity, gender reassignment, marital status, nationality, pregnancy, race and ethnic origin, religion and belief, sex, sexual orientation and socio-economic background.

4. Definitions

Term	Definition
------	------------

Business Continuity Management (BCM)	A holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats might cause, providing a framework for building organisational resilience (ISO 22301:2019).
Business Continuity Management System (BCMS)	The complete set of policies, procedures, plans, and organisational structures for BCM.
Business Impact Analysis (BIA)	A systematic process to identify and evaluate critical processes, their dependencies, and the impacts of disruption.
Business Continuity Plan (BCP)	Documented procedures that guide organisations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.
Incident Management Plan (IMP)	The University-wide framework and procedures for coordinating response to incidents, including command structures and communications protocols.
Risk and Business Continuity Steering Group (RBCSG)	The governance body providing oversight of the BCMS, chaired by the Deputy President (Operations).
Maximum Tolerable Period of Disruption (MTPD)	The time it would take for adverse impacts arising from not providing a service to become unacceptable.
Recovery Time Objective (RTO)	The target time set for recovery of a critical process following an incident.
Recovery Point Objective (RPO)	The maximum tolerable period for data loss.
Gold / Silver / Bronze Command Structure	The University's tiered incident command structure. Gold provides strategic direction and is chaired by the Gold Commander (typically the Deputy President, Operations or nominated deputy). Silver manages tactical coordination and is chaired by the Chair of Silver (typically the Chief Operating Officer or nominated deputy). Bronze provides operational support at site or service level. The structure is activated and stood down in accordance with the Incident Management Plan.

5. Policy

5.1. Purpose

The BCM aims are to:

- Provide a consistent BCMS framework across all Schools, Professional Services and shared services, supporting compliance with legal and regulatory requirements.
- Complement the University's Risk Management framework by identifying and planning for high-impact scenarios where BCM is the appropriate mitigation strategy.
- Formalise critical service priorities and minimum service levels during disruption, and ensure critical processes are recovered before their non-performance threatens the institution.
- Ensure effective planning, training, testing, and continuous improvement to manage operational incidents.
- Identify and mitigate business continuity risk, including supply chain resilience and NHS estate dependencies.
- Promote a resilience culture embedded in strategy, management systems, change control, annual business planning, and staff values and behaviours.

5.2. Scope

The BCMS covers all services across City St George's, University of London, including:

- All University campus sites
- Schools and their supporting specialist facilities, including clinical skills and simulation facilities
- All Professional and Academic Support Services
- Outsourced provision and shared services
- University-owned, operated, maintained, and insured buildings
- NHS-occupied or NHS-maintained estate used by the University, including Hunter Wing and associated facilities, as well as relevant academic partner institutions and placement providers where continuity of service delivery is dependent on their operations.

5.3. Principles

By operating a BCMS aligned to ISO 22301:2019, City St George's Senior Leadership Team is committed to:

- Establishing robust incident response and continuity arrangements to keep students, staff and visitors safe, and to protect the continuity of teaching and research.
- Ensuring effective, timely and coordinated communications during times of disruption.
- Ensuring the University has appropriate and rehearsed arrangements to detect, respond to, and recover time-sensitive and essential activities impacted by significant disruption.
- Identifying and planning for high-impact scenarios where BCM is the appropriate risk mitigation strategy.
- Understanding cross-site and NHS estate dependencies to reduce silos and deepen the management of risk.
- Operating a managed system to report, debrief and learn from incidents, to continually improve response and resilience.
- Ensuring resilience considerations are embedded into project change control and procurement so that new areas of risk are not introduced without appropriate understanding and mitigation.

5.4. Roles and responsibilities

Role	Responsibility
Council	Receives annual assurance on the state of BCM readiness.
Audit and Risk Committee (ARC)	Receives annual assurance on the state of BCM readiness and scrutinises BCM arrangements on behalf of Council.
Senior Leadership Team (SLT)	Overarching responsibility for the Policy and its implementation. Receives lessons learnt reports for major incidents.
Deputy President (Operations) (DP(O))	Executive lead for BCM. Chairs RBCSG. Responsible for the Incident Management Plan (IMP) and overall BCM programme.
Risk and Business Continuity Steering Group (RBCSG)	Governance oversight of the BCMS. Approves lessons learnt reports, BCP updates, and risk register inclusions. Reports quarterly to SLT.
Risk and Business Continuity Manager	Day-to-day BCMS operation; incidents log maintenance; debrief coordination; exercise facilitation and testing; bi-monthly RBCSG reporting.
School COOs / Professional Service Directors	Responsible and accountable for school and departmental BCPs. Annual review and assurance to RBCSG.
Gold Commander	Gold Commander provides strategic direction during incidents.
Chair of Silver	Chair of Silver leads tactical coordination, including communications and operational decisions, consulting the Gold Commander as necessary.
Bronze Commanders	Bronze Commanders manage operational response at site or service level. Roles are activated in accordance with the Incident Management Plan.

6. Procedure

The BCMS operates through the following key procedures:

6.1. Business Impact Analysis

Each School and Professional Service will conduct a BIA to identify critical processes, their dependencies, recovery time objectives, and the impacts of disruption. BIA results are analysed to identify the focus of BCPs, single points of failure, and risk acceptance levels.

6.2. Business Continuity Plans

Critical processes identified through Business Impact Analyses (BIAs) will guide the development of Business Continuity Plans (BCPs), incorporating appropriate mitigation and recovery strategies.

BCPs are required for all organisational areas responsible for delivering critical activities, including academic schools, professional services, and key operational functions where disruption would have a material impact on the University's ability to deliver its strategic, regulatory, or student-facing obligations.

Plans will be reviewed annually and following any major incident. All BCPs are stored on the Business Continuity SharePoint Hub.

6.3. Incident Management

The University Incident Management Plan provides the framework for coordinating response to incidents. The IMP is managed centrally and is the responsibility of the DP(O) and RBCSG. It is supported by threat-specific and consequence management plans, building-specific plans, and service BCPs.

6.4. Root Cause Analysis and Lessons Learnt

All Silver and above incidents will be subject to a formal debrief and root cause analysis process. Lessons learnt must be recorded in 4Risk and tracked to closure via the Business Continuity Incidents Log and Action Tracker.

6.5. Testing and Exercising

BCPs will be tested through table-top exercises and scenario-based testing to validate command structures, communications protocols, and recovery procedures. Testing is planned on a prioritised and risk-based schedule. Testing completion is monitored and reported to RBCSG quarterly. In addition, all Silver and above incidents are subject to a formal lessons-learned exercise.

6.6. NHS Estate Dependencies

Where the University occupies or relies upon NHS-owned or NHS-maintained estate (including Hunter Wing, Tooting Campus), continuity arrangements must account for the dependency on a third-party landlord and infrastructure.

Formal Memoranda of Understanding (MoUs) with NHS Trust partners will define respective responsibilities and continuity obligations. Pending the establishment of formal MoUs, interim

arrangements are in place, including agreed responsibility matrices and operational protocols, which support coordination and continuity of service delivery across shared estate and services.

These arrangements are subject to review and oversight by the Risk and Business Continuity Steering Group (RBCSG).

6.7. Risk Appetite Alignment

Business Continuity Management (BCM) operates as a key control mechanism within the University's Risk Management Framework and supports the management of risks in line with the approved Risk Appetite Statement.

Business continuity arrangements are required where:

- The potential impact of disruption exceeds defined risk appetite thresholds
- The Maximum Tolerable Period of Disruption (MTPD) for a service is short relative to its criticality
- Failure to deliver a service would result in material regulatory, financial, safety, or reputational consequences

Recovery objectives defined through Business Impact Analysis (BIA), including Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), must be proportionate to the University's risk appetite and aligned to the tolerance levels agreed for critical services.

Where residual risk remains outside appetite:

- This must be explicitly documented within the relevant risk register
- Escalation must be made via the Risk and Business Continuity Steering Group (RBCSG)
- Formal acceptance must be approved at the appropriate governance level

BCM therefore provides assurance that the University can operate within its defined risk appetite during periods of disruption.

6.8. Assurance and Oversight

The University applies a Three Lines of Defence model to provide assurance over the effectiveness of Business Continuity Management:

First Line (Operational Management): Schools and Professional Services are responsible for maintaining Business Impact Analyses (BIAs) and Business Continuity Plans (BCPs), ensuring plans are current, tested, and embedded within local operations, and for identifying and managing continuity risks within their areas.

Second Line (Risk and BCM Function): The Risk and Business Continuity function provides oversight by setting BCM policy, standards, and guidance; monitoring compliance with BCMS requirements; reviewing BIA/BCP quality and testing outcomes; and maintaining the central incident log, action tracker, and reporting to RBCSG.

Third Line (Independent Assurance): Internal Audit provides independent assurance by reviewing the design and effectiveness of the BCMS, assessing governance, controls, and compliance with policy, and reporting findings to the Audit and Risk Committee (ARC).

This model ensures a structured and auditable approach to resilience across the institution.

6.9. Incident Response and Recovery Lifecycle

The University manages incidents through a structured lifecycle to ensure clarity of roles, decision-making, and recovery:

- Detection and Escalation: Identification of a disruption and activation of appropriate response structures (Bronze, Silver, Gold)
- Response and Stabilisation: Immediate actions taken to protect life, safety, and critical operations
- Continuity and Service Recovery: Implementation of Business Continuity Plans to maintain or restore critical services within agreed tolerances (MTPD/RTO)
- Recovery and Restoration: Transition from continuity arrangements to a stable operating state, which may include a revised new normal
- Review and Improvement: Formal debrief, root cause analysis, and tracking of lessons learnt through 4Risk to completion

Clear transition points between Incident Management and Business Continuity must be maintained to ensure effective coordination throughout.

6.10. Incident Communications

Effective communication during incidents is critical to maintaining trust, safety, and operational effectiveness. The University adopts a structured communication approach based on:

- Single Source of Truth: All incident information is coordinated centrally to ensure consistency and accuracy
- Defined Authority: Communications are led by the Chair of Silver (or delegated authority), consulting the Gold Commander as necessary, and supported by Communications teams
- Operational communications (staff and students): clear, timely, action-focused
- Strategic communications (SLT, Council): concise, risk-informed updates
- External communications (regulators, partners, media): controlled, accurate, and compliant

Communication protocols must align with regulatory requirements, including timely notification to bodies such as the Office for Students (OfS) and, where relevant, the Information Commissioner's Office (ICO).

6.11. Third-Party and NHS Estate Dependencies

Where the University relies on third-party infrastructure, including NHS-owned or NHS-managed estate, Business Continuity Plans must explicitly account for these dependencies. This includes:

- Identification of critical services reliant on external infrastructure
- Clear understanding of roles and responsibilities between the University and third-party providers
- Defined escalation routes and communication protocols during incidents
- Alignment of continuity arrangements with partner organisations

Formal agreements, including Memoranda of Understanding (MoUs), Service Level Agreements (SLAs), or responsibility matrices, must be established where appropriate. Where such agreements are not yet formalised:

- Interim arrangements must be documented
- Risks must be recorded and actively managed through the risk register
- Oversight must be provided via the RBCSG

This ensures continuity risks arising from external dependencies are understood, controlled, and subject to governance oversight.

7. Advice and Guidance

For advice and guidance regarding business continuity management, please contact the Risk and Business Continuity Manager via the Business Continuity SharePoint Hub. [City St George's - Incident Management and Business Continuity](#)

All Business Continuity documentation, templates, and supporting materials are held on the Business Continuity SharePoint Hub with restricted access for designated BCM personnel.

8. Legal and Regulatory Responsibilities

Martyn's Law (Terrorism (Protection of Premises) Act 2025) places statutory duties on the University as an Enhanced Tier premises to have in place public protection procedures covering evacuation, invacuation, lockdown and communication, and where applicable public protection measures to reduce vulnerability to terrorism. The University as a corporate body is the Responsible Person under the Act, with the President holding overall accountability and the Deputy President, Operations as the senior delegated lead. Governance for Martyn's Law is integrated within the University's existing health and safety governance structure, with compliance reported through the University Health and Safety and Wellbeing Committee to the Audit and Risk Committee (ARC). Detailed governance, delegation, operational procedures, and risk register position are set out in the University's dedicated Martyn's Law policy and procedures.

Where a Martyn's Law-related event activates the BCM framework, the BCM Silver structure provides supporting governance for incident response coordination. The Risk and Business Continuity Manager is responsible for ensuring BCM plans appropriately cross-reference relevant public protection procedures.

9. Failure to Comply

Failure to comply with this policy may result in:

- Inadequate preparedness to respond to and recover from incidents, potentially resulting in significant operational, financial, legal, and reputational damage to the University.
- Non-compliance with regulatory requirements including Office for Students (OfS) expectations regarding business continuity and risk management.
- Disciplinary action in accordance with university policies for staff who fail to fulfil their designated BCM responsibilities.
- Escalation to the RBCSG, Audit and Risk Committee (ARC), and Senior Leadership Team where Schools or Professional Services fail to maintain current BCPs or provide required assurance.

10. Review

This policy is reviewed annually by the Risk and Business Continuity Manager in consultation with the RBCSG or following a major incident. Changes are approved by the Audit and Risk Committee (ARC) on the recommendation of Senior Leadership Team (SLT).

Who reviews the policy	Risk and Business Continuity Manager
Review frequency	Annually, or following a major incident
Who approves the policy	Audit and Risk Committee (ARC), on the recommendation of Senior Leadership Team (SLT)

Policy Information

Should you require further information regarding this policy or access to the policy in an alternative format, then please contact the Risk and Business Continuity Manager, Legal, Governance, Risk and Compliance.

Policy Title:	Business Continuity Policy
Policy Version:	2.0
Status:	Approved
Primary Author:	Risk and Business Continuity Manager
Related Policies:	Risk Management Policy, Incident Management Plan, Flexible Working Policy, Acceptable Use of IT Policy, Health and Safety Policy, Martyn's Law Policy and Procedures (pending)
Accountable Authority:	Deputy President, Operations
Approving Authority:	Audit and Risk Committee (ARC)
Date of Approval:	09 June 2026
Policy effective from:	09 June 2026
Date of Review:	12 months from approval date, or following a major incident

APPENDICES

Appendix A – Key Performance Targets

Five metrics are used to monitor the currency of the BCMS and are reported to the RBCSG quarterly:

KPI	Target / Description	Reporting Frequency
Training	90% of staff with an identified BCMS role will have completed the Introduction to Business Continuity training with an 80% pass mark.	Quarterly to RBCSG
BIA / BCP Currency	Key services will have a Business Impact Analysis and Business Continuity Plan in place, updated within the last 12 months.	Quarterly to RBCSG
Testing and Exercising	In line with a prioritised and documented annual exercise schedule.	Quarterly to RBCSG
Supply Chain	Contracts register updated for critical contracts; records of expiry inform re-tendering; standard terms and conditions applied.	Quarterly to RBCSG
Incidents	All Silver incidents debriefed within 28 days of stand-down. All resilience improvement actions tracked to completion via the Business Continuity Incidents Log and Action Tracker.	Quarterly to RBCSG

Appendix B – Supporting Documentation

The following documents support this policy and are held on the Business Continuity SharePoint Hub:

- Incident Management Plan
- BCM Root Cause Analysis and Lessons Learned Process
- Business Continuity Incidents Log and Action Tracker
- BIA and BCP Templates
- Lessons Learnt Report Templates
- Debrief Meeting Agenda Template
- MOU with St George's University Hospitals NHS Foundation Trust (Tooting Campus) – in development
- Annual Business Continuity Report to SLT and Audit and Risk Committee (ARC)
- Martyn's Law – Written Delegation Instrument (pending)
- Martyn's Law – Public Protection Procedures (pending)
- Martyn's Law – Vulnerability Assessment and SIA Audit Log (pending)
- Martyn's Law – Staff Training and Awareness Programme (pending)

Note: Supporting documents have restricted access and are held centrally on the Business Continuity SharePoint Hub, in addition to being held locally in Schools and departments.