IT Services Policy

DG23 – Computer Room Operation Policy

Prepared by: <Shelim Miah>
Version: 2.0
Effective Date: June 2020  
Next Review: June 2023

Reviewers:
Kathy Whelan, IT Service Desk Manager
Aqib Khan, Network Operations Manager
David Pick, Network Security
Henrik Brogger, Head of Service Delivery
Martin Evans, Head of Data Centre Services
Mike Wearden, Head of Networks
Chris walker, Research consultant
Martin Evans, Head of Data Centre Services
Alex Owen, Physics
Haris Krikelis, Research Systems Support
Jonathan Croft, Wolfson IT Manager
Thomas King, AD for Research

Policy Owner:
Name/Position  Rachel Bence – CIO IT Services

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Author</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initial version.</td>
<td>William Mordaunt</td>
<td>23/03/2010</td>
</tr>
<tr>
<td>1</td>
<td>Annual Review – No change</td>
<td>Tavinder Jhandu</td>
<td>08/04/2014</td>
</tr>
<tr>
<td>1</td>
<td>Annual Review – No change</td>
<td>Tavinder Jhandu</td>
<td>14/08/2015</td>
</tr>
<tr>
<td>1</td>
<td>Initial version.</td>
<td>William Mordaunt</td>
<td>23/03/2010</td>
</tr>
<tr>
<td>1.1</td>
<td>Transferred onto a Policy Template</td>
<td>Shelim Miah</td>
<td>22/03/2016</td>
</tr>
<tr>
<td>1.2</td>
<td>Updated the policy</td>
<td>Shelim Miah</td>
<td>20/01/2020</td>
</tr>
<tr>
<td>1.3</td>
<td>Comments and feedback received</td>
<td>Shelim Miah</td>
<td>24/01/2020</td>
</tr>
<tr>
<td>1.4</td>
<td>Comments from MDEvans</td>
<td>Shelim Miah</td>
<td>14/01/2020</td>
</tr>
<tr>
<td>1.5</td>
<td>Comments from Alex Owen</td>
<td>Shelim Miah</td>
<td>15/04/2020</td>
</tr>
<tr>
<td>1.6</td>
<td>Further review comments</td>
<td>Shelim Miah</td>
<td>28/04/2020</td>
</tr>
<tr>
<td>1.7</td>
<td>Further updates across the whole document</td>
<td>Shelim Miah</td>
<td>28/05/2020</td>
</tr>
<tr>
<td>2.0</td>
<td>Document finalised</td>
<td>Shelim Miah</td>
<td>08/06/2020</td>
</tr>
</tbody>
</table>

Authorisation:

Name / Position  Rachel Bence CIO IT Services
Signature        Rachel Bence
Date             29 June 2020

Queen Mary University of London - Open
CONTENTS

1 POLICY STATEMENT ........................................................................................................... 4
2 SCOPE .................................................................................................................................. 4
3 POLICY DETAIL .................................................................................................................. 4
4 ROLES & RESPONSIBILITY ................................................................................................. 8
5 MONITORING ..................................................................................................................... 8
6 EXCEPTIONS ........................................................................................................................ 8
7 REFERENCES ......................................................................................................................... 8
8 APPENDIX A ........................................................................................................................ 9
1 Policy Statement

1.1 This policy requires that Queen Mary University of London (QMUL) Computer Rooms are managed in a consistent manner with due regard to industry best practice with a view to the systems residing in these rooms being secure, safe and operating efficiently.

1.2 Queen Mary University of London operates a number of Computer rooms across several sites. The Core set of Computer Rooms are operated by IT Services and provide Queen Mary wide services; other Computer rooms may house departmental systems and/or communications equipment.

1.3 This Policy:

- Outlines the expectations and standards of Computer Rooms.
- Provides a consistent approach to operating and maintaining Computer Rooms.
- Provides a policy to maintain the integrity and security of the Systems in these Computer Rooms.
- Outlines roles & responsibilities relating to Computer Rooms

2 Scope

2.1 This policy applies to all IT Computer Rooms owned or rented by Queen Mary including rooms that host local departmental systems, 3rd party data centres and any third party that wishes to access or use these rooms.

2.2 Computer Rooms include; Datacentre, Nodal Rooms, Communications Rooms, local Server Rooms and any room that predominately holds IT infrastructure.

3 Policy Detail

3.1 Security

3.1.1 Computer Rooms house servers, network equipment and other associated hardware that are critical to providing IT services to both staff and students across multiple sites.

3.1.2 These rooms must be protected to ensure business continuity and located in secure areas, which are protected by a physically sound security perimeter.

3.1.3 All doors must be suitably protected against unauthorised access e.g.:

- Swipe access
- Pin access
- lock and key
Multiple levels of protection should be used, dependent upon the vulnerability of the location; the importance of the services that they run and the value of the equipment and data held there

3.1.4 Access to Computer Rooms must be controlled and restricted to authorised personnel only.

3.1.5 Department Heads or where delegated department managers must ensure local procedures are in place to maintain and update authorisation to access Computer Rooms.

3.1.6 Authorised personnel must accompany visitors to Computer Rooms at all times. A record must be maintained of their arrival and departure times for rooms that host critical IT infrastructure.

3.1.7 Datacentre Rooms must be monitored by intruder detection systems and where practical, CCTV, monitored by security staff.

3.1.8 Entrances to Nodal and Communication Rooms where possible should be visible on CCTV to ensure that any attempt of forced entry or unauthorised access is captured.

3.1.9 All staff and visitors requiring access to Computer Rooms must be made aware of the security requirements and any emergency procedures in effect.

3.1.10 No food or drink is to be taken or consumed in any Computer Room.

3.2 Environmental Controls

3.2.1 When selecting a Computer Room, the following should be considered:

- Location, whether the room gets warm quickly
- Exposure to floods, fires and any other hazards should be taken into account
- Windowless to avoid heat from exposure to the sun
- Appropriate air volume for circulation must be provided suitable for the use of the space

3.2.2 IT infrastructure equipment must be stored in their own dedicated rooms. Where there are multiple resilient and redundant elements of IT hardware (servers, network switches etc.) they should be strategically placed, so there is space between equipment to allow diverse routings of cables and avoids exposure to heat from the adjacent IT equipment.

3.2.3 Computer Rooms must have appropriate cooling systems to prevent the overheating of IT infrastructure equipment. This may include passive or free-air solutions, scaled for the planned as well as current needs of the space.

3.2.4 Computer Rooms with critical IT infrastructure equipment must have cooling systems designed to eliminate a single point of failure.

3.2.5 Temperature and humidity must be monitored in the rooms with critical IT infrastructure equipment. Where the measurements are discovered to fall outside the normal operating ranges, corrective action must be taken promptly.
3.2.6 All Computer Rooms must be equipped with ceiling mounted smoke detectors.

3.2.7 Computer Rooms with critical IT infrastructure must have in addition to smoke detectors; fire detection measures such as heat detectors, automatic fire suppression systems that all provide automatic alerts to individuals responsible for the IT infrastructure and or maintenance of the Computer Room to take the appropriate remedial action.

3.2.8 Computer Rooms with critical IT infrastructure must have flood detection system that provide alerts.

3.2.9 Critical IT infrastructure must be protected from power failure and fluctuation by an uninterruptible power supply (UPS), which should be maintained and replaced when necessary.

3.2.10 The material used for the flooring should be aligned with the underlying raised floor tiles to facilitate access to the under floor area if available.

3.2.11 The floor surface should be vinyl tiles or similar material to avoid the accumulation of dust.

3.2.12 The Floor loading limits should be known and must not be exceeded.

3.2.13 IT Computer Room doors should be at least 42 inches (1.06m) wide and eight feet (2.4m) tall to allow easy installation of large IT equipment.

3.2.14 Equipment in the core set of Computer Rooms must be housed in purpose-made equipment racks and have adequate grounding to prevent electric shock.

3.2.15 The equipment racks should be braced to reduce the potential of IT equipment from falling and causing damage or injury.

3.2.16 Where equipment racks have integrated doors they must be used unless the equipment does not fit or the doors are no longer operational. Where doors are fitted and are operational, these must be kept closed unless access to the equipment is required.

3.2.17 All racks and IT equipment must be clearly labelled to help track the IT equipment owner or person responsible.

3.2.18 A record or log must be maintained that details the; location, IT equipment owner and location of racks and IT equipment held within Computer Rooms.

3.2.19 There should be at least 4 feet (1.2m) wide aisle between adjacent rows of racks to allow individuals to safely work and manoeuvre.

3.2.20 IT Computer Rooms must have a maintenance regime in place to ensure that IT Computer Rooms are working at the appropriate operating level and any defects, wear and tear or issues are identified and treated accordingly.

3.2.21 Each Computer Room must have a designated ‘owner or accountable person’ to oversee and manage the room’s usage.
3.3 **Health & Safety**

3.3.1 The IT Computer Room owner is responsible for managing risks to health and safety through risk assessment and control measures.

3.3.2 Staff have a duty to report any health and safety incidents or concerns to the IT Computer Room owner or accountable person.

3.3.3 Training requirements must be determined for all staff wishing to work in the area and reviewed on at most an annual basis.

3.3.4 Staff have a duty to inform management of any training needs to allow them to work safely within IT Computer Rooms.

3.3.5 Computer Rooms housing critical IT Infrastructure equipment must not be used for storage. Other Computer Rooms should not be used for storage except for limited storage of non-flammable items in metal cupboards. Cardboard boxes, paper and flammable materials must not be stored in Computer Rooms except for time limited purposes of installing or removing equipment.

3.3.6 When planning installation or refurbishment work, the room must be checked for the presence of Asbestos before commencing any work.

3.3.7 Fire stoppers must be in place to prevent the spread of a fire, for any installation or refurbishment work that has resulted in drilling of holes in walls.

3.3.8 Computer Room owners must ensure that sufficient instructions/checklists/procedures are available and close to hand with defined actions on what to do during an emergency and lone working.
4 Roles & Responsibility

4.1 Department Heads or where delegated department managers are to ensure associated processes and guidance documents are available to staff using their rooms, which includes the process for authorising access to IT Computer Rooms.

4.2 The Risk and Governance Manager will be responsible for initiating the review cycle for the policy, process document owner to carry out the review. The Document owner will assess and incorporate any comments or feedback received.

4.3 Once the document has been updated, the Risk and Governance Manager will take the document to the appropriate board for approval. All approved documentation are to be stored in a central repository and uploaded to the web where applicable.

4.4 The Computer Room owner is responsible for implementing and enforcing the requirements set out in this Policy. They are also responsible for devising and implementing any remedial actions to ensure that their Computer Room is compliant with this policy.

5 Monitoring

5.1 IT Services may request checks to be carried out as part of internal audits, any findings will reported to the IT Lead Team (ITLT) for any corrective actions to be issued.

5.2 Where non-compliance is identified and the corrective actions have not been implemented, ITS will take appropriate action, which may result in escalation to senior management.

6 Exceptions

6.1 Where an exception to this policy is required, the matter should firstly be referred to the ITLT to assess the exception.

6.2 The ITLT will then make a decision or refer this to the IT Strategy Board (ITSB) for a decision.

7 References

SOP DG23 – Computer Room Operation Standard Operating Procedures
QMUL Records Retention Policy and Schedule
DG00 Review and Update of Policies -
https://www.its.qmul.ac.uk/media/its/documents/governance/sops/DG00-Review--Update-of-Policies--V2.0.pdf
## Appendix A

### 8.1 Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Rooms</td>
<td>Computer Rooms is a broad terminology that refers to; data centre, nodal room, communications rooms, server room and any room that solely holds IT infrastructure</td>
</tr>
<tr>
<td>Data Centre</td>
<td>Core Server room that hosts applications and data that provide QMUL wide services</td>
</tr>
<tr>
<td>Nodal Rooms</td>
<td>The Core set of Computer Rooms are operated by IT Services and house servers and other equipment that facilitate the services to a building.</td>
</tr>
<tr>
<td>Communication Rooms</td>
<td>Computer Rooms that hosts IT equipment that facilitate services to a particular section or floor of a building</td>
</tr>
<tr>
<td>Local Server rooms</td>
<td>The Computer Rooms, which are operated by IT Services, house departmental systems and/or communications equipment.</td>
</tr>
<tr>
<td>IT Infrastructure equipment</td>
<td>IT components or equipment such Servers, Network Switches, routers, software etc. that underpin a service. This does not include, USB, laptops, removable devices et.</td>
</tr>
<tr>
<td>Critical IT Infrastructure</td>
<td>IT equipment that is essential for the operation of the IT Services, Computer Rooms that house essential IT equipment that were they to fail, IT services would no longer be available.</td>
</tr>
<tr>
<td>User</td>
<td>A member of staff, enrolled student, contractor, visitor, or another (any other) person authorised to access and use QMUL’s systems.</td>
</tr>
<tr>
<td>ITLT</td>
<td>IT Lead Team – Team of Senior Managers consisting of the Assistant Directors of IT, Faculty Relationship Managers and Chaired by the IT Director.</td>
</tr>
<tr>
<td>ITSB</td>
<td>IT Strategy Board – Team of Executive Managers consisting of Vice Principals and the IT Director, who oversee the delivery of the IT Strategy.</td>
</tr>
</tbody>
</table>