IT Services Policy Document

Secure Desk Working Policy

Prepared by: <Shelim Miah>
Version: 1.0
**Effective Date:** 19/12/2019

**Review Date:** 15/01/2021

**Reviewers:**
- Kathy Whelan, IT Service Desk Manager
- Henrik Brogger, Head of Service Delivery
- David Pick, Network Security
- David Boakes, Assistant Director ITS Operations
- Madalyn Hardaker, SMD, Information Governance Lead

**Policy Owner:**
Name/Position: Rachel Bence, Chief Information Officer

**Revision History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Author</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Initial version.</td>
<td>Shelim Miah</td>
<td>19/06/2019</td>
</tr>
<tr>
<td>0.2</td>
<td>Feedback and comments</td>
<td>Shelim Miah</td>
<td>02/10/2019</td>
</tr>
<tr>
<td>0.3</td>
<td>Feedback and Comments</td>
<td>Madalyn Hardaker</td>
<td>04/11/2019</td>
</tr>
<tr>
<td>0.4</td>
<td>Title Change</td>
<td>Shelim Miah</td>
<td>04/12/2019</td>
</tr>
</tbody>
</table>

**Authorisation:**

<table>
<thead>
<tr>
<th>Name / Position</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rachel Bence</td>
<td>Rachel Bence</td>
<td>13/12/2019</td>
</tr>
</tbody>
</table>
1 Policy Statement

1.1 The Secure Desk Working Policy helps to prevent unauthorised access to QMUL assets in all media forms and IT equipment. With the aim of preserving the confidentiality, integrity and availability of sensitive information and assets. This is achieved by ensuring that users remove sensitive information and securing assets from their work area when not in use or when they leave their workstation to reduce the risk of security breaches in the workplace.

1.2 The Policy aims to:

- Reduce the risk of compromising information
- Outline the roles & responsibilities of users
- Ensure QMUL information is controlled and accessible to those authorised to do so
- Promote a healthier and safe working environment

2 Scope

2.1 This Policy is applicable to all QMUL users and their affiliates who have access to QMUL information, assets or IT equipment. All QMUL users are required to protect any assets that may contain sensitive information kept at their desk/workstation either temporarily or permanently and covers records in all media formats including but not limited to:

- Paper
- Electronic documents
- Emails
- Visual images such as work related photographs
- Audio and video tapes, CDs, DVDs and cassettes
- Memory sticks
- Portable and mobile devices (laptops/IPad/Tablets/Phones etc.) and hard drives
- Databases
- Whiteboards
3 Policy Detail

3.1 Users are responsible for ensuring sensitive information in their work area is secure at all times, whether in hardcopy or electronic form.

3.2 Information not in use must be either physically locked away or electronically secured i.e. Lock screens, and must not be left unattended, especially information of a personal or sensitive nature.

3.3 Computer desk/workstations, portable and mobile device screens must be locked when unattended to help reduce the risk of information being seen by unauthorised users. This includes periods when users are away from their desk for meetings, lunch, retrieving printing etc. unless the work area can be secured e.g. locked office.

3.4 Cabinets containing information, keys or equipment must be closed and locked when not in use or unattended.

3.5 Keys for cabinets or computer rooms must not be left unattended.

3.6 Mobile and portable devices when not in use must be either locked with a locking cable or locked away in a drawer when not in use.

3.7 At the end of the working day, computer desk/workstations, laptops and or any work related devices are completely shut down unless requested otherwise and all information assets are secured.

3.8 Information captured on whiteboards should be erased once its purpose has been fulfilled.

3.9 Users should be aware of the position of their screen. Wherever possible, ensure that unauthorised people cannot see the screens, especially when viewing personal or sensitive information.

4 Roles & Responsibilities

4.1 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.

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

5 Process and Procedures

5.1 The associated processes and guidance documents can be found by visiting the ITS webpage.

6 Monitoring

6.1 It is mandatory for all QMUL users to comply with this IT Policy and any associated procedure. Where non-compliance is identified, ITS will take appropriate action, which may result in escalation to senior management for action to be taken.

6.2 Checks will be made by the Risk and Governance Manager and the findings will be reported to the IT Lead Team (ITLT) in the first instance for corrective actions to be issued.

6.3 The Assistant Director of IT Operations, in conjunction with the Risk & Governance Manager, is responsible for the monitoring, revision and updating of this policy.
7 Exceptions

7.1 In the event of an exception that is not addressed by this policy, the matter will be firstly referred to the ITLT via the Assistant Director for IT Operations.

7.2 The ITLT will then make a decision or refer this to the IT Strategy Board (ITSB) for further guidance as necessary.

8 References

8.1 NHS Digital Clear Desk and Screen Policy
8.2 SANS Clear Desk Policy
## Appendix A – Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>A set of rules, guidance or framework that outlines the boundaries in which to operate. Policies are the guidelines under which processes and Procedures are developed. The Policy address who is responsible for the execution and enforcement of the Policy, and why the Policy is required.</td>
</tr>
<tr>
<td>Process</td>
<td>The process is the high level view or the map of tasks involved in delivering an outcome. Processes address who is responsible to perform the Process (department, division), what major functions are performed, and when the function is triggered.</td>
</tr>
<tr>
<td>Procedure</td>
<td>Procedures define the specific instructions necessary to perform a task or part of a Process. Procedures detail who performs the task, what steps are performed and when the steps are performed. They can take the form of a work instruction, such as a desk top Procedure or a quick reference guide.</td>
</tr>
<tr>
<td>QMSE</td>
<td>The Queen Mary Senior Executive team is Queen Mary’s senior management team and comprises the Principal, Vice-Principals and the Senior Officers in Professional Services who advise the Principal on the management of day-to-day College business as well as its long-term future.</td>
</tr>
<tr>
<td>ITSIB</td>
<td>The IT Implementation Strategy Board (ITSIB) is the overarching governance board for IT Services and has responsible for the delivery of the IT Strategy.</td>
</tr>
<tr>
<td>ITLT</td>
<td>IT Lead Team (ITLT) The IT Lead Team are responsible for developing and implementing the IT services Strategy that enables the department to deliver on service improvement.</td>
</tr>
<tr>
<td>Policy Owner</td>
<td>The person responsible for the maintenance and updating of the Policy.</td>
</tr>
<tr>
<td>Sensitive Information</td>
<td>Information that could harm, embarrass or affect the reputations of an individual or organisation if it were released or seen by others.</td>
</tr>
<tr>
<td>Personal Information</td>
<td>Information that can identify a living person e.g. names, photographs, biometrics, CCTV etc. It applies to student, parent and staff data.</td>
</tr>
<tr>
<td>Work Environment</td>
<td>This includes any work space used to carry out your work e.g. desk, worktops, assembly room, store rooms pedestal, shelves and cabinets to store your work or devices etc.</td>
</tr>
<tr>
<td>Locked</td>
<td>Where screen locked is referenced this relates to device running but screensaver or lock screen is engaged and a password is required to unlock the device. Where devices is locked away is referenced, this refers to the device being physically locked against physical removal.</td>
</tr>
</tbody>
</table>