IT Services Policy

IS01 Information Security and Acceptable Use Policy

Prepared by: Rhianne Short
Version: 2.0
Last Review Date: N/A   Next Review Date: 28/03/2024

Reviewers: ITLT, (IGG), Jonathon Croft (Barts Cancer Institute), Research Information Governance Group (RIGG)

Policy Owner: Rachel Bence, Chief Information Officer, IT Services

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Author</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial version.</td>
<td>Rhianne Short</td>
<td>28/03/2023</td>
</tr>
<tr>
<td>2.0</td>
<td>Update</td>
<td>Rhianne Short</td>
<td>27/07/2023</td>
</tr>
</tbody>
</table>

Authorisation:

<table>
<thead>
<tr>
<th>Name / Position</th>
<th>Rachel Bence, Chief Information Officer, IT Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td>R.Bence</td>
</tr>
<tr>
<td>Date</td>
<td>27/07/2023</td>
</tr>
</tbody>
</table>

Superseded Policies

<table>
<thead>
<tr>
<th>Ref</th>
<th>Policy Title</th>
<th>Date Superseded</th>
</tr>
</thead>
<tbody>
<tr>
<td>DG18</td>
<td>Password Management Policy</td>
<td>28/03/2023</td>
</tr>
<tr>
<td>DG20</td>
<td>Access to and Use of Email Policy</td>
<td>28/03/2023</td>
</tr>
<tr>
<td>DG29</td>
<td>Acceptable Use of IT Policy</td>
<td>28/03/2023</td>
</tr>
<tr>
<td>N/A</td>
<td>Secure Desk Working Policy</td>
<td>28/03/2023</td>
</tr>
</tbody>
</table>
Contents

1 QUEEN MARY INFORMATION SECURITY OBJECTIVE .................................................. 4
2 SCOPE ......................................................................................................................... 4
3 TERMINOLOGY ........................................................................................................... 4
4 USE OF QMUL OWNED DEVICES ............................................................................ 5
5 BRING YOUR OWN DEVICE (BYOD) ........................................................................ 5
6 INTERNET & NETWORK USE ..................................................................................... 6
7 EMAIL ACCESS & USE ............................................................................................... 7
8 PASSWORD MANAGEMENT ......................................................................................... 7
9 CLEAR DESK & LOCKED SCREEN ............................................................................. 8
10 REMOVABLE MEDIA ................................................................................................. 9
11 REMOTE WORKING ................................................................................................... 10
12 REPORTING SECURITY INCIDENTS .......................................................................... 10
13 TRAINING .................................................................................................................. 11
14 MONITORING ............................................................................................................ 11
15 RELATED DOCUMENTS ............................................................................................ 11
16 REFERENCES .............................................................................................................. 12
17 APPENDIX A - LEGAL AND POLICY STATEMENT .................................................... 12
1 Queen Mary Information Security Objective

1.1 Queen Mary University of London (QMUL) is an institution of research and learning and is heavily dependent on using information in all forms. Protecting its information assets and the IT systems on which these are processed, stored, or transmitted will help enable the University to fulfil its mission, comply with legislation, protect its reputation, and ensure that a high-quality service can continue to be offered to our students, employees, and alumni. The Policy provides safeguards for staff and for our information resources, but it does not seek to restrict academic freedom.

1.2 It is QMUL’s policy to protect its information and information systems from the loss of confidentiality, integrity, and availability. This requires that all our employees are appropriately aware of, and comply with, QMUL’s Information Security Policy.

1.3 QMUL’s security objective is to protect the University from cyber and information security issues that might have an adverse impact on fulfilling its mission and ensuring that a high-quality service can continue to be offered to students, employees, and alumni. All employees & students have a responsibility to help protect QMUL information and technology.

1.4 The objective of this new policy (for superseded policies please see table on page 2) is to ensure that all employees with access to QMUL’s information resources, IT systems and services understand the rules and their responsibilities of using, accessing, or interacting with them, whether provided by central IT or by any other department of QMUL.

2 Scope

2.1 This policy applies to all employees, QMUL affiliates, agency employees, contractors, and Post-Graduate Research students (hereby referred to as ‘employees’), who are provided with access to information assets, facilities, and systems, including computers, applications, and networks, owned, or operated by QMUL.

2.2 This policy covers all locations including remote workers and overseas campuses.

2.3 This policy does not apply to Undergraduate and Post Graduate Taught students.

2.4 This policy covers the use of IT owned and issued by QMUL, the use of personal devices and accessing information from third-party devices, in reference to QMUL and its activities, and other technologies owned by QMUL.

2.5 This policy applies to QMUL information in all forms, wherever it is created, collected, processed, shared, stored, or destroyed.

2.6 This policy supersedes:
   - DG20 – Access to and Use of Email
   - DG29 – Acceptable Use of IT
   - DG18 – Password Management Policy

3 Terminology

3.1 The following terms will be used throughout the policy:
   - Shall; is used to state a mandatory requirement of this policy.
   - Should; is used to state a recommended requirement of this policy.
• QMUL owned devices; is used in reference to QMUL owned and ITS managed, and QMUL owned and self-managed devices.

4 Use of QMUL Owned Devices

The following statements apply to all employees using QMUL owned devices:

4.1 All employees shall recognise the need to protect QMUL information that is stored on or accessed using a QMUL device.

4.2 Employees shall not load data or software that is illegal or in breach of copyright or any other license terms onto QMUL owned devices.

4.3 Devices shall not be:

- “jailbroken” – modified to remove restrictions or policies, e.g. an apple device which is jailbroken to allow apps to be downloaded that are not from the official Apple App Store.
- “rooted” – the process of obtaining privileged access/control, e.g. rooting an Android device to give permissions that enable the user to change the Android software to apple iOS software.
- have any software/firmware installed which is designed to gain access to functionality that the user is not intended to have.

4.4 Portable devices should be kept in a secure location when not in use (see Section 11 for Clear Desk and Locked Screen)

4.5 Employees shall make no attempts to disable or over-ride any of QMUL’s installed configurations or software, including anti-malware software, software firewalls, and automatic updating services.

The following statements apply to all employees using QMUL owned self-managed devices:

4.6 Employees shall ensure their devices and applications are kept updated; this can be done automatically by regularly restarting devices (at least weekly).

4.7 A device or applications for which vendor security updates are not available shall not be used for any sort of QMUL business.

4.8 All QMUL devices shall have a password, passcode, or biometric security as default. These security controls shall not be removed.

4.9 Staff should not have email auto-forwarding rules from a QMUL account to a non-QMUL account.

4.10 This policy reflects the Legal and Policy statement that all employees agree to when logging in to a QMUL managed device (Appendix A).

5 Bring Your Own Device (BYOD)

5.1 Employees using their own device to access any QMUL related information should have a passcode or biometric security if available. Jailbroken or rooted devices are strictly prohibited.
Employees must not circumvent security controls (definitions and examples of “jailbroken” and “rooted” can be found in statement 4.3 of this policy).

5.2 All employees shall protect QMUL information that is stored on or accessed using BYOD, including but not limited to taking adequate measures to secure the device. For example, using anti-virus software, multi-factor authentication, using a VPN.

5.3 Employees shall ensure their devices and applications are kept updated. A device and applications for which supplier updates are not available shall not be used for any sort of QMUL business.

5.4 Following the ending of employment with QMUL, employees shall delete all QMUL data and associated applications from the BYOD device.

6 Internet & Network Use

6.1 Use of Internet/intranet/e-mail/instant messaging may be subject to monitoring for reasons of security and/or network management and users may have their usage of these resources subjected to limitations by QMUL.

6.2 The use of organisational computer resources is subject to local jurisdiction law (including international laws) and any abuse will be dealt with in line with the QMUL Discipline Policy and Procedure (https://hr.QMUL.ac.uk/media/hr/policies/Discipline-Policy-Updated-2021.pdf)

6.3 Unless in the pursuit of occupational research and education activities that have been explicitly authorised by QMUL, employees shall not visit Internet sites using QMUL accounts or QMUL owned devices that contain obscene, hateful, extremist, or other objectionable material, and shall not make or post indecent remarks, proposals, or materials on the Internet. As stated in QMUL’s Legal & Policy Statement (Appendix A) users must also not process, publish, create, store, download, distribute or transmit material or data that is:

- Prohibited by UK or other governing jurisdiction law.
- Extremist
- Discriminatory or defamatory.
- Harassing or threatening.
- Derogatory to any individual or group.
- Obscene or pornographic.
- Likely to bring QMUL into disrepute.

6.4 Employees shall not download from the internet or install on any QMUL owned computer or device any software for which QMUL does not have a valid license, is of an illegal or malicious nature, or poses a security threat to the organisation.

6.5 The use of social media shall be in accordance with QMUL Social Media Guidance and Freedom of Speech Policy (https://arcs.QMUL.ac.uk/media/arcs/policyzone/Freedom-of-Speech-June-2019.pdf)

6.6 Employees shall not intentionally interfere in the normal operation of the QMUL IT environment or take any steps that hinder others in their use of the QMUL IT environment, and will not
examine, change, or use another person’s files or any other information asset for which they do not have the owner’s explicit permission.

6.7 QMUL reserve the right to block any content that poses a risk to QMUL’s network, or contains obscene, hateful, or other objectionable material (see 6.3 for further detail).

7 Email Access & Use

7.1 All employees shall use the QMUL-provided email system predominantly for conducting QMUL business. Moderate personal use is permitted as long as it does not contradict other sections of this policy.

7.2 Email is less secure than other communication channels and shall not be used to send sensitive data or information, see Data Matrix (DG09 Information Classification Policy, appendix B https://www.its.qmul.ac.uk/media/its/documents/governance/sops/DG09-Information-Classification-Policy-V3.1.pdf) for guidance on how each classification of data can be sent.

7.3 Employees shall not open incoming e-mail attachments or click on hyperlinks that originate with unknown third parties. These may contain malware and any such e-mails must be reported to report-phishing@QMUL.ac.uk (see section 14 for reporting security incidents).

7.4 Emails that originate from outside of QMUL have an ‘external’ marking. All employees should be vigilant in engaging with ‘external’ marked emails, especially if they appear to be from a known colleague as it could be a fraudulent email impersonating a colleague.

7.5 Employees shall check the destination addresses of messages before sending to ensure that the message contents and any attachment complies with the Information Classification Policy (DG09, https://www.its.QMUL.ac.uk/media/its/documents/governance/sops/DG09-Information-Classification-Policy-V3.1.pdf), to prevent accidental data breaches.

7.6 QMUL retains the right to add/remove access to shared mailboxes or ‘Send As’ permissions to reflect a change of job role or responsibilities.

8 Password Management

8.1 All employees shall have an IT account with a unique username and password to access IT services.

8.2 Employees shall not directly, or indirectly, allow another person to use their credentials, including colleagues or IT technicians. IT Service Desk employees shall not request employees to disclose their passwords when providing support or investigating problems.

8.3 Passwords shall not be written down or reproduced in any way, other than in a QMUL approved password manager. IT Security team has guidance on approved Password Managers, this guidance can be found on the Information Security website (https://www.its.qmul.ac.uk/cybersecurity/information-security/password-managers)

8.4 It is not mandatory that passwords be changed frequently. All employees, however, shall change their passwords whenever there is any indication of possible system or password compromise and report such instances to the IT Service Desk. If IT Service Desk or the Information Security Team
receive indicators of account compromise the effected accounts will be required to change passwords.

8.5 When choosing a password, employees should ensure it is strong. The following can increase the strength of a password:

- Not based on anything that could be easily guessed using personal related information, e.g. names, telephone numbers, dates or birth, vehicle registrations, etc.
- Free of repeating identical, all-numeric or all-alphabetic characters.
- Be at a minimum 12 characters or longer.
- Avoid using special characters.
- Using the three random words technique to help users create less predictable passwords. ([https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words](https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words))

8.6 Employees shall not include passwords in any personal automated logon processes (e.g. scripts, macros, etc.)

8.7 Employees shall not use the same password for QMUL accounts and personal accounts.

8.8 Employees shall avoid replicating the same password across different accounts, systems, and services as a compromise on one account could mean all accounts and services are compromised. This does not include systems that use Single Sign On (SSO), as SSO allows a single QMUL account to be used across several systems.

9 Clear Desk & Locked Screen

9.1 Hot desking areas shall be left clean, tidy, and neat when unoccupied, and at the end of each working day. Wastepaper, litter, etc. must all be removed to allow the workstations to be cleaned and to enable others to use the workstation if necessary.

9.2 Individual offices shall be locked (where possible) when unoccupied and documents shall be secured when not in use.

9.3 All confidential documents must be removed from desks, stored, and locked in lockable furniture (e.g., filing cabinets and drawers), when not in use. Where this is not achievable in a remote working setting, practical steps may be taken to ensure documents remain ‘out of reach’ and ‘out of sight.’ see Data Matrix (DG09 Information Classification Policy, appendix B ([https://www.its.qmul.ac.uk/media/its/documents/governance/sops/DG09-Information-Classification-Policy-V3.1.pdf](https://www.its.qmul.ac.uk/media/its/documents/governance/sops/DG09-Information-Classification-Policy-V3.1.pdf)) for guidance on how each classification of data can be stored.

9.4 Mobile (laptops, smartphones, and tablets) and removable media devices (USBs etc.) shall be secured with appropriate physical security measures (e.g. lockable storage) when not in use. Keys or codes for accessing secure lockable furniture must not be left unattended at the desk.

9.5 Unattended desktops and mobile devices shall be left in a secure state when working in a shared or public space; this means manually applying the ‘screen lock.’ This means as a minimum applying
9.6 Employees shall manually log out of shared equipment in meeting and teaching rooms when no longer in use, such as shared PCs attached to screens or Surface Hubs.

9.7 All wastepaper which contains confidential information, as defined in the DG09 Information Classification Policy, shall be shredded by placing in designated secure waste units provided on campus and in office buildings (DG09 Information Classification Policy https://www.its.qmul.ac.uk/media/its/documents/governance/sops/DG09-Information-Classification-Policy-V3.1.pdf).

9.8 Employees should be vigilant to the security of their workstation, considering any such risks before commencing work e.g., potential for sensitive conversations to be overheard or sensitive information to be seen by passing colleagues. Such risks are greater when working in public places and connecting to public networks e.g., trains and cafes.

9.9 Confidential documents, mobile and removable media devices shall not be left unattended, including USB sticks.

9.10 Employees should ensure that they ‘leave’ Microsoft Teams meetings at the end of the meeting. Any subsequent conversation may be recording or being listened to by attendees without your knowledge.

10 Removable Media

10.1 Employees should avoid using a removable media device, such as USB sticks, where possible and Microsoft One Drive used instead.

10.2 Employees should ensure that if using a removable media device, no one else has used the device and they are aware of exactly what is contained on the device.

10.3 Removable media devices should not be used for Confidential data as defined in the DG09 Information Classification Policy (https://www.its.qmul.ac.uk/media/its/documents/governance/sops/DG09-Information-Classification-Policy-V3.1.pdf).

10.4 Removable media devices should be encrypted.

10.5 Where information is stored on mobile devices or removable media, special care shall be taken to ensure that the device is protected from theft, loss, or damage.

10.6 If there is a university requirement for using a removable media device and a new device is required, this should be procured through IT Services to ensure that it is secure, by contacting the IT Service desk (see 12.2 for IT Service Desk contact details).

10.7 Damaged or faulty removable media devices must not be used, and any fault reported to the IT Service desk (see 12.2 for IT Service Desk contact details).

10.8 If a removable media device needs to be disposed, IT Service desk shall be contacted to advise on how to dispose securely (see 12.2 for IT Service Desk contact details).
11 Remote Working

11.1 Remote working is defined as any work that is conducted on behalf of QMUL by an Employee whilst not on University premises. For example, working from home, on trains, in cafes, etc.

11.2 All employees have a responsibility to protect the information and assets of QMUL, and those entrusted to QMUL by third parties, in their possession to the same standard as when on QMUL premises.

11.3 In remote working conditions, QMUL information must not be shared with unauthorised persons and any hard copies or removable media must be returned to QMUL for disposal using the designated secure waste units provided. Under no circumstances should this information be placed in regular waste bins at the remote location or at QMUL.

11.4 If working remotely employees must ensure that the same standard of security is applied to documents as when on QMUL premises. (See DG09 Information Classification Policy).

11.5 Employees must be able to justify the movement of protectively marked physical documents outside of secure locations. Unless there is a necessary reason for the movement and/or transfer of such documents, documents should be kept in secure premises.

11.6 Employees should take steps to ensure that the remote working environment offers a suitable level of privacy (i.e. from other individuals in the vicinity being able to view papers or screens being worked on or being able to overhear private conversations) before working on any Sensitive Information.

11.7 For further information on remote working please see QMUL’s remote working policies - https://hr.QMUL.ac.uk/temporary-remote-working/policies-procedures-and-guidance-during-remote-working/.

12 Reporting Security Incidents

12.1 Employees shall report any suspected or actual breaches of any information or compromises to IT systems promptly to the IT Service Desk. This includes:
   • theft, or loss of QMUL information or QMUL’s IT systems, including computers, portable devices, storage devices or documents containing QMUL information.
   • suspicious calls or requests for information.
   • suspicious external devices attached to your computer, for example USB stick.
   • signs of unauthorised access, for example unexplained pop-ups or requests for credentials.
   • signs of an unknown programme running.
   • system unexpectedly running extremely slowly.

12.2 Employees can contact the IT Service Desk using the live chat system - https://QMUL.bomgarcloud.com/, raising a ticket on the self-service portal https://servicedesk.QMUL.ac.uk/ or calling the IT Service Desk 24/7 on 020 7882 8888

12.3 Any suspected phishing attacks shall be reported to the Information Security Team at report-phishing@QMUL.ac.uk.
12.4 When raising a ticket to report the theft or loss of personal, confidential, or financial information, the contents of this information should not be included.

13 Training

13.1 All employees shall complete mandatory Cyber Security and GDPR training (login to https://cloud.metacompliance.com for training).

13.2 Line managers shall monitor Cyber Security and GDPR training compliance.

14 Monitoring

14.1 Line Managers shall monitor employees’ compliance with this policy.

14.2 Where non-compliance is identified ITS will take action under the applicable policies.

14.3 Independent reviews of this policy will be conducted by both Internal and External Auditors on a periodic basis.

The Assistant Director - Office of the Chief Information Officer, in conjunction with the Head of Information Security, is responsible for the monitoring, revision and updating of this document.

15 Related Documents

15.1 ITS Policies https://www.its.qmul.ac.uk/governance/policies/

15.2 (DG09) Information Classification Policy (https://www.its.qmul.ac.uk/media/its/documents/governance/sops/DG09-Information-Classification-Policy-V3.1.pdf)

15.3 QMUL Discipline Policy and Procedure (https://hr.qmul.ac.uk/media/hr/policies/Discipline-Policy-Updated-2021.pdf)

15.4 (DG09, Appendix B) Data Matrix (https://www.its.qmul.ac.uk/media/its/documents/governance/sops/DG09-Information-Classification-Policy-V3.1.pdf)

15.5 Guidance for Staff on the Use of Social Media (https://hr.qmul.ac.uk/media/hr/docs/Social-Media-Guidance-for-Staff_February-2020.pdf)

15.6 Information on Compliance with the Freedom of Information Act at Queen Mary University of London (https://foi.qmul.ac.uk/#:~:text=Members%20of%20the%20public%20now,and%20receive%20copies%20of%20information)

15.7 Data Protection Policy (https://arcs.qmul.ac.uk/media/arcs/policyzone/Data-Protection-Policy-v03.0.pdf)
16 References


17 Appendix A - Legal and Policy Statement

Access
Access to any data, program, or other information on Queen Mary University of London (QMUL) systems must be authorised by QMUL. It is a criminal offence to obtain unauthorised access or make unauthorised modifications to this computer system. QMUL may refer any unauthorised access to appropriate authorities. Unauthorised users may be subject to CRIMINAL PROSECUTION AND/OR CIVIL ACTION OR QMUL DISCIPLINARY PROCEEDINGS.

Use
Users must not process, publish, create, store, download, distribute or transmit material or data that is:

- Prohibited by UK law.
- Extremist
- Discriminatory or defamatory
- Harassing or threatening.
- Derogatory to any individual or group.
- Obscene or pornographic.
- Engaged in any purpose that is illegal or contrary to QMUL policy or business interests.
- Likely to bring QMUL into disrepute.

Monitoring
Queen Mary University of London monitors its IT systems for the purposes of Operational Integrity, Policy Enforcement and Crime Prevention.