# IS01 Information Security and Acceptable Use Policy

## 1. Purpose

1.1. Queen Mary University of London (Queen Mary, the University) is an institution of research and learning and is heavily dependent on using information in all forms. Protecting the institution's 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 the University's policy to protect its information and information systems from compromise of confidentiality, integrity, or availability. This requires that all our employees are appropriately aware of, and comply with, the University's Information Security Policy.

1.3. The University'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 the University information and technology.

1.4. The objective of this policy (for superseded policies please see *Policy Information and Document Control* table) is to ensure that all employees with access to the University 's information resources, IT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 the University.

1.5. The Policy aims to:

- Outline the expectations of system managers
- Ensure a consistent approach to capturing and storing security incidents, including logging and monitoring related information

1.6. The University's policy is that user activities, system errors and information security events must be monitored and recorded in logs which are subsequently protected against unauthorised changes.

## 2. Legislative context

2.1. The University s Information Security Management System (ISMS) is aligned to the requirements of the International Standard ISO 27001: 2022. This is recognised as best practice in information security management. This policy is aligned with the ISMS Legal Register. See also Appendix A – Legal and Policy Statement

## 3. Terminology

The following terms will be used throughout the policy:

- Must is used to state a **mandatory** requirement of this policy
- Must not is used to state a **prohibition** of this policy
- Should is used to state a **recommendation** of this policy

## 4. Scope

4.1. This policy applies to all employees, University affiliates, agency employees, contractors/vendors, visitors, partners and Postgraduate 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 the University.

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

4.3. This policy does not apply to Undergraduate and Postgraduate Taught students.

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

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

4.6. This policy reflects the Legal and Policy statement that all employees agree to when logging in to the University managed device.

## 5. Use of University-Owned Devices

The following statements apply to all employees using University-owned devices:

5.1. All employees must recognise the need to protect the University's information that is stored on or accessed using a University device.

5.2. Employees must not load data or software that is illegal or in breach of copyright or any other license terms onto the University-owned devices.

5.3. Devices must not:

- be "jailbroken" or "rooted" – 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
- have any software/firmware installed which is designed to gain access to unintended/unsupported functionality

5.4. Portable devices should be password protected and kept in a secure location when not in use (see Section 10 *Clear Desk & Locked Screen*)

5.5. Employees must make no attempts to disable or over-ride any of the University's installed configurations or software, including anti-malware software, security tooling, software firewalls, and automatic updating services.

5.6. Standard devices must not be transported into *High-Risk Countries* as defined in IS14 policy. An alternative the University Loan PC may be provided for travel and access from within those countries with only browser access to limited applications. Users must consult IS14-Staff-travelling-to-high-risk-countries and request a University Loan PC device through a Service Desk request.

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

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

5.8. A device or applications for which vendor security updates are not available must not be used for any sort of University business.

5.9. All the University devices must have a password, passcode, or biometric security as default. These security controls must not be removed.

5.10. Staff must not enable email auto-forwarding rules from a University account to a non-University account. See https://www.qmul.ac.uk/governance-and-legal-services/media/arcs/governance/information-governance/data-protection/GDPR-Update-3---Oct-2020.pdf

## 6. Bring Your Own Device

The following statements apply to all employees using personal devices treated as Bring Your Own Device (BYOD):

6.1. Employees using their own device to access any University-related information must 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 5.3 of this Policy).

6.2. Any unsupported operating system must not be used. The following are supported operating systems and can be used, providing their versions still receive security updates: Windows, iOS, Android, Linux, macOS.

6.3. Employees must ensure their devices and applications are kept updated. Any device or applications for which supplier updates are no longer available must not be used for any sort of University business.

6.4. All employees must protect University information that is stored on or accessed using BYOD, including but not limited to taking adequate measures to secure the device. This should include as a minimum, using anti-virus software, multi-factor authentication, using a VPN when accessing University systems or data using public Wi-Fi, and applying full disk encryption to the device.

6.5. Upon the ending of employment or contract with the University, employees and other personnel must securely delete all the University data and associated applications from the BYOD and confirm in writing to their line manager that this has been completed.

## 7. Internet & Network Use

7.1. 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 the University.

7.2. 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 University Discipline Policy and Procedure.

7.3. Unless in the pursuit of occupational research and education activities that have been explicitly authorised by the Research Ethics Committee, employees must not visit Internet sites using the University accounts or the University-owned devices

that contain obscene, hateful, extremist, or other objectionable material, and must not make or post indecent remarks, proposals, or materials on the Internet. As stated in the University'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
- Engaged in any purpose that is illegal or contrary to the University policy or business interests
- Likely to bring the University into disrepute

7.4. Employees must not download from the internet or install on any University-owned computer or device, any software for which the University does not have a valid licence, is of an illegal or malicious nature, or poses a security threat to the organisation.

7.5. The Ideas Forum is the governance group through which requests for new software or vendor engagements must be raised. This ensures that relevant information and enterprise architecture artifacts are developed in support of the Information Security Management System.

7.6. The use of social media must be in accordance with the University Social Media Guidance and Freedom of Speech Policy

7.7. Employees must not intentionally interfere in the normal operation of the University IT environment or take any steps that hinder others in their use of the University 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.

7.8. The University reserves the right to block any content that poses a risk to the University's network, or contains obscene, hateful, or other objectionable material.

## 8. Email Access & Use

8.1. All employees must use the University-provided email system for conducting University business. Moderate personal use is permitted as long as it does not contradict other sections of this policy.

8.2. Email is less secure than other communication channels and must not be used to send sensitive data or information, see Information Storage Matrix (DG09 Information Classification Policy, appendix B) for guidance on how each classification of data can be sent.

8.3. Employees must 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 should be reported whenever possible through the "Report Message" button in Outlook, else by forwarding to report-phishing@qmul.ac.uk (see section 13 for reporting security incidents).

8.4. Emails that originate from outside of the University have an 'external' marking. All employees should be vigilant in engaging with 'external'-marked emails, especially if they appear to be from a mailbox named after a colleague. Use of public email services for the impersonation of colleagues is commonly observed in scams.

8.5. Employees must check the destination addresses of messages before sending to ensure that the message contents and any attachment comply with the DG09 Information Classification Policy to prevent accidental data breaches.

8.6. The University reserves the right to add/remove access to shared mailboxes or 'Send As' permissions to reflect a change of job role or responsibilities.

8.7. Employees should access their emails through the Microsoft Outlook applications and web client where possible.

## 9. Password management and multi-factor authentication

9.1. All employees must be issued an IT account with a unique username and password to access IT services.

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

9.3. Passwords must not be written down or reproduced in any way, other than in a University-approved password manager. The University Information Security team provides guidance on approved password managers, which can be found on the

Information Security website (https://www.its.qmul.ac.uk/cybersecurity/information-security/password-managers)

9.4. It is not mandatory that passwords be changed frequently. All employees, however, must change their passwords whenever there is any indication of possible system or password compromise and report such instances to the IT Service Desk (see section 13 of this policy). If IT Service Desk or the Information Security Team receive indicators of account compromise, the affected accounts will be required to change passwords.

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

- Avoiding anything that could be easily guessed using personal related information, e.g. names, telephone numbers, dates or birth, vehicle registrations, etc.
- Avoid repeating identical, all-numeric or all-alphabetic characters
- Choosing a password with a minimum of 12 characters, or longer. Password length is more important than password complexity
- The University recommends using the three random words technique to help create less-predictable passwords. (https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words)
- If your laptop supports PIN login, this must be a minimum strength of 8 digits. This must not be based on easily guessable information (such as your date of birth)

9.6. Employees must not use the same password for University accounts and personal accounts.

9.7. Employees must not re-use 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 University account to be used across several systems.

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

9.9. Employees must use Multi-Factor Authentication (MFA) to secure sign-ins to all applications, unless it is not available for an application. Where MFA is unavailable for an application, this must be reported in order to be recorded on the institutional cyber risk register, and the service owner will be required to manage alternative compensating security controls.

## 10. Clear Desk & Locked Screen

10.1. Hot desking areas must be left clean, tidy and neat when unoccupied. Wastepaper, litter, etc. must all be removed to allow the workstations to be cleaned and to enable others to use the workstation if necessary.

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

10.3. 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) for guidance on how each classification of data can be stored.

10.4. Mobile (laptops, smartphones, and tablets) and removable media devices (USBs etc.) must 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.

10.5. Unattended desktops and mobile devices must be locked and left in a secure state when working in a shared or public space; this means manually applying the 'screen lock.' (To lock Windows devices, press Windows key & L key. For macOS devices press ctrl-Command-Q).

10.6. Employees must 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.

10.7. All wastepaper which contains confidential information, as defined in the DG09 Information Classification Policy, must be shredded by placing in designated secure waste units provided on campus and in office buildings

10.8. 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.

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

10.10. Employees must ensure that they exit Microsoft Teams meetings at the end of the meeting. Any subsequent conversation may be recording or being listened to by attendees without your knowledge.

## 11. Removable Media

11.1. Employees should avoid using removable media devices, such as USB sticks, where possible, and use the institutional Microsoft OneDrive service instead.

11.2. 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 13.2 for IT Service Desk contact details).

11.3. Removable media devices, or the data they contain, should be encrypted.

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

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

11.6. Removable media devices must only be used as permitted by DG09 Information Classification Policy.

11.7. Damaged or faulty removable media devices must not be used, and any fault reported to the IT Service Desk (see 13.2 for IT Service Desk contact details).

11.8. If a removable media device requires secure disposal, IT Service Desk must be contacted to advise on how to dispose securely.

## 12. Remote Working

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

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

12.3. In remote working conditions, the University information must not be shared with unauthorised persons, and any hard copies or removable media must be returned to the University for disposal using the designated secure waste units provided.

Under no circumstances must this information be placed in regular waste bins at the remote location or at the University.

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

12.5. 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.

12.6. 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 or being able to overhear private conversations) before working on any sensitive information.

12.7. For further information on remote working please see the University's hybrid working policy and procedure.

## 13. Reporting Security Incidents

13.1. Employees must 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 the University information, or the University's IT systems, including computers, portable devices, storage devices or documents containing the University information
- suspicious calls or requests for information
- suspicious external devices attached to your computer, for example, a 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

13.2. Employees can contact the IT Service Desk using the live chat system - https://chat.its.qmul.ac.uk , by raising a self-service ticket at https://servicedesk.qmul.ac.uk, or by calling the IT Service Desk 24/7 on 020 7882 8888.

13.3. Any suspected phishing incidents must be reported using the Report button in Outlook. If this is not possible, please send to report-phishing@qmul.ac.uk.

13.4. When raising a Service Desk Incident to report the theft or loss of personal, confidential, or financial information, the contents of this information must not be included.

## 14. Training

14.1. All employees must complete mandatory Cyber Security and GDPR training, which can be found by logging in to https://cpd-training.qmul.ac.uk/.

14.2. All staff who have access to staff or student personal data must also be required to complete refresher training annually, in line with the University schedule of mandatory training at https://www.qmul.ac.uk/human-resources/organisational-professional-development/queen-mary-essentials/mandatory-training/.

14.3. Line managers must monitor Cyber Security and GDPR training compliance.

## 15. Monitoring

15.1. Line Managers must monitor employees' compliance with this policy.

15.2. Where non-compliance is identified ITS should be alerted and will take action under the applicable policies.

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

15.4. The Chief Information Security Officer, in conjunction with the Governance, Risk and Compliance Manager, is responsible for the monitoring, revision and updating of this policy.

## 16. Exceptions

16.1. Any exception to this policy must be documented with business reasoning and signed off by the University's Chief Information Officer along with the Chief Information Security Officer, before it is taken forward.

## Appendix A – Legal and Policy Statement

### Access

Access to any data, program, or other information on Queen Mary University of London (the University) systems must be authorised by the University and is subject to the IS01 Information Security & Acceptable Use Policy. It is a criminal offence to obtain unauthorised access or make unauthorised modifications to this computer system. The University may refer any unauthorised access to appropriate authorities. Unauthorised users may be subject to CRIMINAL PROSECUTION AND/OR CIVIL ACTION OR UNIVERSITY 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 the University policy or business interests
- Likely to bring the University into disrepute

### Monitoring

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

## Policy Information and Document Control

| | |
|---|---|
| **Policy title** | IS01 Information Security and Acceptable Use Policy |
| **Version number** | V3.3 |
| **Related policies and procedures** | **1.** ITS Policies including ISMS policies<br>**2.** Data Protection Policy<br>**3.** DG09 Information Classification Policy; Appendix B Information Storage Matrix<br>**4.** Information on Compliance with the Freedom of Information Act at Queen Mary University of London: https://foi.qmul.ac.uk/<br>**5.** Queen Mary Discipline Policy and Procedure:<br>**6.** Guidance for Staff on the Use of Social Media:<br>**7.** Guidelines on the Right to Privacy and the Monitoring of Data: |
| **Superseded policies** | DG18 Password Management Policy<br>DG20 Access and Use of Email Policy<br>DG29 Acceptable Use of IT Policy |
| | |
| **Approval level** | Information Governance Group |
| **Approval date** | 15th January 2025 |
| **Last Review Date** | 6th July, 2026 |
| | |
| **Next full review due** | January 2029 |
| | |
| **Policy owner** | Rachel Bence, Chief Information Officer, IT Services |
| **Policy contact** | Ambrose Neville – Chief Information Security Officer |

## Version Control

| Version | Date | Reason for updates/Summary of key changes |
|---|---|---|
| **1.0** | 28/03/2023 | Initial Version |
| **2.0** | 27/07/2023 | Updates |
| **3.0** | 12/12/2024 | Annual review, transfer to new template |
| **3.1** | 08/01/2026 | Annual review for the PSG 2026 review. Minor updates include the use of 'Must' instead of 'Shall' as per the University Policy Writing Guide. |
| **3.2** | 28/01/2026 | Minor updates to correct the numbering and references within the document |
| **3.3** | 03/07/2026 | Minor update to address PIN strength |
| **3.4** | 06/07/2026 | Minor updates to the text. Removed references to archived links and other typing errors. |