

Joiners, Movers & Leavers 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.
- 1.2. The over-arching Information Security and Acceptable Use Policy (IS01) describes The University's overall security objectives and associated policy objectives.
- 1.3. This policy (Joiners, Movers & Leavers Policy) outlines the appropriate security controls which will be implemented to ensure that security is maintained when users of University information assets join, move or leave their role within Queen Mary.

2. Legislative and regulatory context

- 2.1. Queen Mary'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

- 3.1. 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.

5. Principles

- 5.1. The University's policy is that users' (as defined in 4.1) access to its information assets must be limited to what they need in order to fulfil their roles. This applies to joiners as much as it does to existing members of staff.
- 5.2. Care must be taken to ensure that staff who change role within the University do not retain permissions from any previous role for longer than is necessary. The permissions of leavers must be removed when they stop being employed by the University or, for non-employees such as alumni and students, when their contract ends.

6. Roles and responsibilities

- 6.1. Human Resources is responsible for ensuring this policy is adhered to for both joiners and leavers.
- 6.2. Individual line managers are responsible for ensuring compliance with the policy for people who change role. In addition, line managers are responsible for contractors/vendors and the related onboarding/offboarding procedures.

7. Recruitment and screening

- 7.1. As part of the recruitment process, Human Resources must ensure the following screening checks are completed for all members of staff:
 - Identity checks / legal right to work
 - Satisfactory reference / employment checks
 - Background / vetting checks

- Qualifications / membership checks (if relevant for the role)
- 7.2. Particular scrutiny should be given to roles which will afford privileged access to University resources, such as administrators of IT systems.
- 7.3. If any issues are identified during the screening process which could mean a candidate who has been given a conditional offer of employment may not be suitable for their role, a decision must be made between Human Resources and the individual manager about whether to proceed with an appointment.

8. Terms and Conditions of Employment

- 8.1. All employees and users of University IT resources must be informed that they are required to abide by the University's policies relating to data protection and information security and must sign contractual agreements which state their responsibilities relating to information security.
- 8.2. By signing the contractual agreement, employees and users of University IT resources make a formal undertaking to abide by the policies. This undertaking applies both during and after their employment or other contract at the University.

9. Movers

- 9.1. If an employee moves to a role internally which will involve a change in the information resource, they have access to (whether increased or reduced), it must be the responsibility of the new line manager to ensure that:
- Additional access or equipment required for the new role is in place in a timely manner through informing ITS Service Desk
 - Access to equipment and information assets used in the previous role which is no longer required is revoked through informing ITS Service Desk and any physical assets returned
- 9.2. The process for assigning access to movers will follow the principle of leaving and starting, i.e. removal of all current access rights and provision of access required for the new role.
- 9.3. The previous line manager is required to make arrangements to remove the access privileges related to the staff member's original role.
- 9.4. Human Resources are informed if there may be a requirement for further background screening in the new position, such as when the mover will gain privileged access to information resources.
- 9.5. The above requirements must be reflected in a standard process.

10. Leavers

- 10.1. Upon a staff member leaving, and no later than 24 hours following the end of their last day of employment, the line manager must:
 - Ensure that access to all accounts, including privileged accounts, has been removed.
 - Ensure that all University-owned equipment and information assets (laptops and ID badge for example) have been returned.
- 10.2. Remind exiting employees of their enduring confidentiality agreement obligations.
- 10.3. Where staff leave the organisation, and rejoin later in a new role, new accounts must be issued. Additionally it must be confirmed that any previous accounts have been deactivated before providing access to the new account.
- 10.4. For students and alumni, refer to the Retention [Schedule](#) & Policy

11. Compliance and discipline

- 11.1. Throughout their employment or engagement, all employees this policy applies to must comply with all the University information security policies and procedures.
- 11.2. The University's disciplinary procedures must outline the actions to be taken if an employee or other user disregards the University's information security requirements. The consequences of an information breach and non-compliant activities must be clearly communicated.

12. Monitoring

- 12.1. Compliance with the policies and procedures laid out in this document must be monitored by the Information Security Team as directed by the Head of Information Security, along with independent reviews by both internal and external auditors on a periodic basis.
- 12.2. The Governance Risk and Compliance Manager in conjunction with the Head of Information Security, is responsible for the monitoring, revision and updating of this document.
- 12.3. The effectiveness of this document must be evaluated at monthly information

security meetings and by the Information Governance Group well as the annual review with the Audit & Risk Committee.

13. Exceptions

- 13.1. Any exception to this policy must be documented with business reasoning and signed off by the University's Chief Information Officer and the Head of Information Security before being taken forward.

14. Associated information

- 14.1. Accompanying the ISMS is a Statement of Applicability. This lists all the requirements of ISO 27001 and states how the University will fulfil them.

15. Review

- 15.1. This policy will be reviewed annually by the ISMS operational team, with a full review by the policy owner every 3 years.
- 15.2. Minor updates to this policy that do not affect the rules, principles or intent of this Code may be approved by the Head of Information Security on behalf of the Information Governance Group.

Policy Information and Document Control

Policy title	ITS: Joiners, Movers and Leavers Policy
Version number	V1.1
Related policies and procedures	IS01 – Information Security & Acceptable Use Policy IS15 Access Control Policy ISMS Statement of Applicability ISMS Legal Register
Superseded policies	n/a
Approval level	Information Governance Group
Approval date	15 th January 2025
Last review date	8 th January 2026
Next review due	January 2029
Policy owner	Rachel Bence - Chief Information Officer
Policy contact	Ambrose Neville - Head of Information Security

Version Control

Version	Date	Reason for updates/Summary of key changes
v1.0	15/01/25	Initial approved version
v1.1	08/01/2026	Periodic review for the PSG 2026 review. Minor updates include the use of 'Must' instead of 'Shall' as per the University Policy Writing Guide.