



IT Services Policy

DG19 – Remote Access Policy

Prepared by: <Devopam Dasgupta>
Version: 2.4

Last Review:	04/08/2026	Next Review:	03/08/2026
Reviewers:	Ambrose Neville, Chief Information Security Officer Devopam Dasgupta, Governance Risk and Compliance Manager		
Policy Owner:			
Name/Position	Rachel Bence, CIO		
Revision History			
Version	Description	Author	Date
1	Initial version.	David Pick	01/06/2010
1	Annual Review – No Change	Ian Douglas	23/04/2014
1.1	Section on Remote Vendor access added	Ian Douglas	16/01/2015
1.2	Additional Clauses added	Ian Douglas	29/05/2015
1.3	Updated to Policy template & reviewed	Shelim Miah	28/11/2016
1.4	Reviewed with David Boakes	Shelim Miah	16/03/2017
2.0	Finalised	Shelim Miah	31/03/2017
2.1	Reviewed	Matthew T	07/02/2024
2.2	Annual Review	Devopam Dasgupta	13/11/2025
2.3	Periodic Review – minor updates in terminologies as per the Policy Writing Guide	Devopam Dasgupta	08/04/2026
2.4	Periodic Review -minor updated to the title of Head of Information Security being changed to Chief Information Security Officer.	Devopam Dasgupta	04/08/2026
Authorisation:			
Name / Position	Rachel Bence, CIO		
Signature	R. Bence		
Date	04/08/2026		

CONTENTS

1	POLICY STATEMENT.....	4
2	SCOPE	4
3	POLICY DETAIL.....	4
4	PROCESS AND PROCEDURES	5
5	MONITORING.....	5
6	EXCEPTIONS	6
7	REFERENCES	6

1 Policy Statement

- 1.1 IT Services (ITS) provides a remote access solution to support students and staff who may work from remote locations. In offering this service ITS must ensure that support is available should users require it. This enables Queen Mary University of London (the University) users to benefit from flexible working practises, distance learning and enhances communications. This policy ensures that remote access is managed and information and IT services are protected.
- 1.2 The policy aims to:
 - Outline the expectations of remote access users.
 - Ensure appropriate controls are in place to protect the University data.
 - Ensure access to remote services are managed
 - Outline roles & responsibilities
 - Enhance communications

2 Scope

- 2.1 The policy applies to all users accessing IT services and the University data from remote locations. It also applies to 3rd party suppliers and IT staff who wish to access users' desktop terminals or IT systems to carry out remedial work.
- 2.2 The phrase "remote access" covers both "mobile users" and "teleworkers". Mobile users work casually from a number of remote locations, using equipment that is either their own or supplied by 3rd parties; the equipment may be a mobile device (smart-phone, PDA, etc.) or a standard computer. Teleworkers have a much more formal arrangement, usually with a University-supplied equipment, to work remotely; the more formal arrangement means that the management of the remote equipment is under the University's control.

3 Policy Detail

- 3.1 Any Remote Access Solution (RAS) used to access Central IT Systems and user terminals must be approved by IT Security and the Domain Team Leads (DTL) group.
- 3.2 Whilst evaluating the RAS solution the group must consider any potential risk of data being compromised, for example data may be stored locally on a public computer. The decision must then be documented whether approved or rejected.
- 3.3 Remote access credentials such as a username and password must not be transferred across a network without encryption, especially the general Internet. They must not be stored "in clear text". Refer to IS18 Cryptographic Controls Policy.
- 3.4 Remote access must have enhanced authentication whether a Virtual Private Network (VPN) or remote session access (e.g. VDI, Thin Linc, RDP etc.) from any non-University or untrusted network.
- 3.5 When remote assistance is required for example when someone is connecting to a device as a local user to resolve or demonstrate the use of an application.

- 3.6 The following four controls must be in place:
- The local user has to take a positive action to enable the remote session
 - The local user must be able to view the actions taken by the remote user
 - The local user must be able to terminate the session at any time
 - Business processes must be in place that reminds the local user to close any application showing sensitive data prior to the remote session being established.
- 3.7 Where a 3rd party vendor requires access in order to provide support to the University as part of a support contract the following controls must also be in place:
- Access to the system or application must be controlled by the University. A member of the University must take a positive action to enable the access
 - All vendor access must be pre-arranged with the University and fall under appropriate change control
 - Access must be for a defined time period only and is not open access
 - Access must be limited to the system or application that the vendor is supporting
 - MFA is enforced for any remote access that uses admin accounts (e.g. for access to the admin portal for a cloud vendor).
- 3.8 Any device that intends to be used for remote access must have a suitable anti-virus with the latest definition updates installed and protected with a Firewall.
- 3.9 Multi Factor Authentication (MFA) is required for remote access to applications or services that contain confidential or restricted data.
- 3.10 ITS must periodically, as technology changes, review and advise on new RAS and the preferred technology strategies for remote access.

4 Process and Procedures

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

5 Monitoring

- 5.1 Compliance with the policies and procedures laid out in this document must be monitored by the Information Security Team as directed by the Chief Information Security Officer, along with independent reviews by both internal and external auditors on a periodic basis.
- 5.2 The effectiveness of this document must be evaluated at Infosec Monthly Meetings as well as the annual management review with Senior Management.
- 5.3 The AD of Student and Staff Support Services, in conjunction with the Chief Information Security Officer and the Governance, Risk and Compliance Manager, is responsible for the monitoring, revision and updating of this policy.

6 Exceptions

- 6.1 Any exception to this policy must be documented with business reasoning and signed off by the University's Chief Information Officer and the Chief Information Security Officer before implementation.

7 References

- DG09 – Information Classification Policy
- IS18 Cryptographic Controls Policy
- IS01 Information Security & Acceptable Use Policy