Queen Mary
University of London

IT Services Policy

DG20 – Email Access & Use

Prepared by: < Shelim Miah>
Version: 2.0

Description & Target Audience: This document outlines the use of electronic mail (email) and messaging services to prevent misuse and the protection of data. This document is aimed at all users both students and staff using QMUL services to send and receive messages.			
Effective Date:	**31/03/2017**	Review Date:	**31/03/2018**

Reviewers:	**Paul Smallcombe, QMUL Records & Compliance Manager** **Ian Douglas, Head of Information Security** **Amit Patel, Head of Service Management** **Martin Evans, Head of Data Centre Services** **Tom Jordaan, Infrastructure Software Officer** **David Boakes, Assistant Director Student & Staff Services**
Policy Owner:	
Name/Position	Katie Friis, Interim Deputy Director IT Services

Revision History

Version	Description	Author	Date
1	Initial version.	David Pick	02/06/2010
1	Annual Review – No Change	Ian Douglas	23/06/2014
1.1	Additional Clauses added	Ian Douglas	29/05/2015
1.2	Template updated	Shelim Miah	17/01/2017
1.3	Review with David Boakes	Shelim Miah	17/03/2017
2.0	Finalised	Shelim Miah	31/03/2017

Authorisation:	
Name / Position	**Katie Friis Interim Deputy Director of IT services**
Signature	**Katie Friis**
Date	**31/10/2016**

CONTENTS

1 Policy Statement

1.1 All Email, attachments and messaging services that are sent and received via Queen Marys University of London's (QMUL) services and systems must adhere to this policy to ensure that these services are not misused or contravene legal regulative legislation; such as human rights or data protection acts.

1.2 The policy aims to:

- Outline the expectations of users sending and receiving messages across QMUL IT services and systems.
- Ensure adequate controls are in place to protect QMUL data.
- Outline the acceptable use of messaging services across IT services and systems
- Outline roles & responsibilities
- Enhance Communications

2 Scope

2.2 The policy applies to all users both student, staff and other authorised users of QMUL email and messaging services and related systems; such as Office 365 Email, Outlook, Lync Instant Messenger, any system that provides the capability to send a message to other users.

3 Policy Detail

3.1 All members of staff and students shall use the QMUL-provided email system for conducting QMUL business.

3.2 Any business message shall be retained in accordance with the College Records Retention Policy and Schedule.

3.3 QMUL permits the moderate personal use of email facilities, due care must be taken when it is necessary for any person who is not the normal user of an email account to have access to messages. It shall be recognised that it is an intrusion under the Human Rights Act and shall be allowed only when the need to do so overrides the degree of intrusion. Any decision to do so shall be documented with the criteria used to make the decision.

3.4 QMUL prohibits the use of its email, messaging services, systems or any affiliated service to circulate, promote, store or publicise; illegal, defamatory, offensive material.

3.5 Email is not a secure service, any Confidential or Restricted information (see DG09 – Information Classification Appendix A) that is sent using email must be encrypted.

3.6 To prevent accidental leakage of information users must check the destination addresses of messages before sending, and ensure that the message contents and any attachment complies with see DG09 – Information Classification especially if the message contains Confidential or Restricted information.

3.7 Users must exercise caution and be vigilant when receiving email as email is easy to forge and often used as part of an attack on computer-based systems or administrative processes. If there is any doubt about the source of a message it should be verified by means other than a further exchange of email.

3.8 The QMUL IT Security Team shall be prepared to act as a disinterested third party in any such cases to reduce the degree of intrusion and ensure that proper logging of the intrusion takes place.

3.9 Users must not knowingly allow anyone else to send email using their accounts except using an approved delegation mechanism (e.g. a senior manager delegating access to their secretary).

3.10 Users will be deemed liable for any email or activity from their accounts.

3.11 Whenever any member of the QMUL is considering publishing an email address, they shall consider if it is more appropriate to publish a personal address or a role-based address.

3.12 Users when leaving QMUL must ensure that due consideration is given to both the disposal or transfer of any filed messages and the handling of any new message that may arrive for that account.

3.13 QMUL cannot guarantee that access to email will be available after leaving the organisation.

3.14 The Out of Office function must be switched on with a suitable message.

3.15 IT Services will maintain up-to-date anti-virus software with a good reputation and use it to scan all messages and attachments passing through the central email systems.

3.16 Reasonable steps must be taken to prevent the propagation of computer viruses by email. Incoming and outgoing email must be routed via central mail hubs (including any services operated by third parties on behalf of QMUL which must run adequate virus detection software)

3.17 IT Services will pass all messages through the central email systems through anti-SPAM filters. Messages identified as SPAM shall be discarded; messages that may potentially be SPAM shall be flagged.

3.18 The email facilities may be used for the transfer of data files as attachments, but large files should be transferred by other means. When messages are filed consideration should be given to removing any attachments. Mailboxes must not be used for storing files that should be stored elsewhere.

3.19 IT Services shall provide advice to users about how to achieve this, and also other “good practices” for the use of email including limiting the number of recipients on replies.

3.20 IT Services shall issue regular reminders to all users of these rules and regulations

4 Process and Procedures

4.1 The associated processes and guidance documents can be found by visiting the ITS webpage, some pages maybe restricted to IT staff.

5 Monitoring

3.21 All documents must comply with this policy. Where non-compliance is identified, ITS will take appropriate action.

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

3.23 The AD of Student and Staff Support Services, in conjunction with the Risk & Governance Manager, is responsible for the; monitoring, revision and updating of this policy.

6 Exceptions

3.24 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 Student & Staff Services.

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

3.26 Where compliance is not possible due to technical, financial or regulative reasons, an exception must be raised to the appropriate group for approval so that it can be recorded as being granted exception to the policy.

7 References

SOP DG20 – Email Access and Use
SOP DG09 – Information Classification
SOP DG17 – User Registration
Regulation Concerning Information Technology
JANET Acceptable Use Policy
QM Records Retention Policy and Schedule SOP DG00 – Review and Update of Policies & Standard Operating Procedures

8 Appendix A – Definitions

Term	Meaning
QMUL	Queen Mary University of London
JANET	Joint Academic Network, the organisation the provides QMUL with Internet connectivity
ITS	IT Services
BYOD	Bring Your Own Device refers to users using their own device (which is not owned or provided to you by QMUL) to access and store QMUL information, whether at the place of work or remotely, typically connecting to the QMUL's Wireless Service.
User	A member of staff, enrolled student, contractor, visitor, or another (any other) person authorised to access and use QMUL's systems.
ITLT	IT Lead Team – Team of Senior Managers consisting of the Assistant Directors of IT, Faculty Relationship Managers and Chaired by the IT Director.
ITSB	IT Strategy Board – Team of Executive Managers consisting of Vice Principals and the IT Director, who oversee the delivery of the IT Strategy.
Policy	A set of rules or framework that outlines the boundaries in which to operate.
Process	A structured set of Activities designed to accomplish a specific Objective. A Process takes one or more defined inputs and turns them into defined outputs
SOP	Standard Operating Procedure is a documented high level step-by-step sequence of Operational activities for adhering to policies that can be replicated across several departments and team.
Procedural Document	A set of low level detailed instruction that specify exactly what steps to follow to carry out an activity. E.g. instructions on how to print.
SPOC	Single Point of Contact; a person that acts the coordinator or focal point of information concerning an activity or program