Queen Mary
University of London

IT Services Policy

DG29 – Acceptable Use of IT

Prepared by: < Shelim Miah>
Version: 2.0

Description & Target Audience: This document outlines how QMUL IT is to be used and QMUL deemed to be acceptable use of its IT equipment. This document is aimed at all Staff & Students who have access to any or all IT equipment.			
Effective Date:	**31/10/16**	Review Date:	**31/11/17**

Reviewers:	**Ian Douglas, Head of IT Security** **Shelim Miah, Risk & Governance Manager** **David Boakes, Assistant Director Student & Staff Services**
Policy Owner:	
Name/Position	Mark Duff, Interim Director of IT Services

Revision History			
Version	Description	Author	Date
1	Initial version.	Ian Douglas	15/03/2014
1.0	Transferred into SOP Template	Shelim Miah	30/06/2015
1.1	Add an additional reference and a definition for reasonable personal use	Alan Hardy	12/11/2015
1.2	Change of template	Shelim Miah	21/09/2016
1.3	Review with David Boakes	Shelim Miah	27/10/2016
2.00	Finalised	Shelim Miah	31/10/2016

Authorisation:	
Name / Position	**Mark Duff/ Interim Director of IT Services**
Signature	**Mark Duff**
Date	**31/10/16**

CONTENTS

1 Policy Statement

1.1 To ensure that anyone who has access to QMUL 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.

1.2 The Policy aims to:

- Outline the expectations of IT system and service users.
- Ensure the security and protection of QMUL data.
- Implement controls to safeguard both users and support staff
- Outline roles & responsibilities
- Enhance communications

2 Scope

2.2 This policy is applicable to all IT users i.e. student, staff, visitors and third parties. All users are responsible for their actions when using QMUL IT services and systems. All users are required to behave in an appropriate manner that complies with legal requirements and will not risk damaging QMUL's reputation

3 Policy Detail

3.1 All users must comply with all appropriate policies relating to the governing of IT Services, irrespective if the services are provided by QMUL or by third parties on behalf of QMUL.

These include, but are not limited to:

- Devices, irrespective of ownership, when connected to the QMUL network or Wi-Fi service
- Services run by Information Technology Services (ITS) all services run by other departments within QMUL
- Services operated by third parties on behalf of QMUL including those services hosted by third party organisations
- Services and systems operated by the QMUL Students' Union.

3.2 Failure to comply with the appropriate policies may lead to QMUL disciplinary procedures being invoked. Serious cases may include dismissal without notice and may expose you to court proceedings and criminal or civil liability as appropriate.

3.3 Users will be held responsible for any claims brought against QMUL and any legal action to which QMUL is, or might be, exposed as a result of unauthorised or inappropriate use.

3.4 Users must respect the copyright and intellectual property rights of all materials and software that are made available by QMUL, service providers or third parties.

3.5 Users must Comply with the Data Protection Policy, in particular the obligation to inform the QMUL Records & Information Compliance Manager of the loss of a sensitive information asset

and comply with any Data Protection Legislation as per the DG05 Information Security Incident Reporting Policy.

3.6 Users must comply with the Computer Misuse Act 1990 which makes computer misuse a criminal offence.

3.7 QMUL is bound by its contractual and licence agreements with third party resources, users are required to comply when using these resources.

3.8 When accessing IT Services users must comply with the JANET Acceptable Use Policy and the JANET Security Policy published by JANET (UK).

3.9 Users must take all reasonable precautions to:

- prevent the introduction of viruses, worms, Trojans or other harmful programs to any system, file or software
- protect data from unauthorised access, alteration or deletion

3.10 Users must only use QMUL systems for QMUL related activities or reasonable personal use. Reasonable personal use is defined as incidental or occasional use which does not:

- disrupt or distract the individual from their work
- restrict the use of systems by other legitimate users
- involve illegal or antisocial activity
- add significantly to running costs or breach IT policies
- sending unsolicited emails (junk Mail) or other advertising mail

3.11 Users must immediately return any QMUL owned equipment or software when requested to do so. N.B. personal data held on QMUL devices may be returned to the user where it is possible to do so. QMUL does NOT guarantee that personal data will be returned.

3.12 Users must promptly report the loss or theft of QMUL IT equipment and/or information asset(s), whether in the users care or not.

3.13 Users must not use material or programs in a way which is unlawful, defamatory or invades someone else's privacy.

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

- Prohibited by UK Law
- Discriminatory or defamatory
- Harassing or threatening
- Derogatory, offensive to any individual or group
- Obscene or pornographic
- Engaged in any purpose that is illegal or contrary to QMUL policies or business interests
- Likely to bring QMUL into disrepute

3.15 Users must not use QMUL IT services in such a way as to risk or cause loss of damage to, or breach confidentiality of data or systems.

3.16 Users must not use IT services in a way that risks bringing QMUL into disrepute including associating QMUL with external facilities or bodies by association.

3.17 Users must not disclose their credentials to others, or use someone else's credentials to access information. Users will be held responsible for any misuse of IT services arising from disclosure of their credentials to others.

3.18 Users must not attempt to circumvent system access, processes or attempt to access IT services at QMUL or elsewhere for which they do not have authorisation or facilitate unauthorised access by others.

3.19 Users must not attempt to circumvent, disable or interfere with any software or systems (such as Antivirus, firewalls or intrusion detection) intended to protect IT Services that may damage or destroy any systems or software provided by QMUL.

3.20 Users must not leave their device unattended that may have access to QMUL data assets without first logging out or locking the screen.

3.21 In the event of suspected misuse of IT services, QMUL reserves the right to suspend user accounts and to inspect, monitor, copy or remove users' files if necessary. QMUL may also disconnect the device from the network to prevent access to IT services without notice while investigations proceed.

3.22 Any cases of misuse, abuse, discovery or suspected inappropriate content (obscene, covered by Child Protection Act, terrorism etc.) must be immediately reported to the IT Service desk and as appropriate will be reported to civil authorities.

4 Process and Procedures

4.1 The associated processes and guidance documents can be found by visiting the IT User Account webpage.

5 Monitoring

5.1 Anyone using an IT Account must comply with IT Policies and any associated procedures. Where non-compliance is identified, ITS will take appropriate action.

5.2 Where any breaches of this or any IT policies are suspected they are to be reported to the IT Service Desk.

5.3 The IT Director, in conjunction with the Risk & Governance Manager, is responsible for the; monitoring, revision and updating of this document.

6 Exceptions

6.1 In the event of an exception that are not addressed by this Policy. The matter will be firstly referred to the IT Lead Team (ITLT) for a decision via the Assistant Director for Student & Staff Services.

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

6.3 Legitimate academic study that may involve defamatory, discriminatory or threatening material, the use of images which may depict violence, the study of hate crime, terrorism related material or research into computer intrusion techniques may be carried out provided appropriate control and measures are in place to prevent any exploitation or offence.

7 References

- SOP DG29 – Acceptable Use of IT
- DG05 Information Security Incident Reporting Policy

8 Appendix A - Definitions

Term	Meaning
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.
Data Controller	The Data Controller is a person, group or organisation (in this case QMUL) who determines the purposes for which and the manner in which any personal data are, or are to be, processed.
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.
Account Sponsor	Can be a line manager or person of authority that is responsible and accountable for an IT Account that has been issued.