IT Services Policy

DG29 – Acceptable Use of IT

Prepared by: <Shelim Miah>
Version: 2.2
Effective Date: 15.02.2021

Review Date: 15.03.2021

Reviewers:
- Chris Lightfoot, Head of Information Security
- Shelim Miah, Risk & Governance Manager
- Henrik Brogger, Head of IT Service Delivery
- Shahid Rashid, Assistant Director Platforms and Services
- Richard Young, Assistant Director Development & Solutions
- Rupa Dey, Assistant Director Projects & Change
- Mike Wearden, head of Infrastructure
- Terry Holland, Servers & Storage Manager
- Skender Osmani, Head of Client Devices
- David Pick Network Security Manager
- Jason Bunning, Head of Enterprise Systems
- Ed Webb, Head of Development Services
- Sundip Lotay, Infrastructure Software Manager

Policy Owner:
Name/Position: Rachel Bence, CIO IT services

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Author</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initial version.</td>
<td>Ian Douglas</td>
<td>15/03/2014</td>
</tr>
<tr>
<td>1.0</td>
<td>Transferred into SOP Template</td>
<td>Shelim Miah</td>
<td>30/06/2015</td>
</tr>
<tr>
<td>1.1</td>
<td>Add an additional reference and a definition for reasonable personal use</td>
<td>Alan Hardy</td>
<td>12/11/2015</td>
</tr>
<tr>
<td>1.2</td>
<td>Change of template</td>
<td>Shelim Miah</td>
<td>21/09/2016</td>
</tr>
<tr>
<td>1.3</td>
<td>Review with David Boakes</td>
<td>Shelim Miah</td>
<td>27/10/2016</td>
</tr>
<tr>
<td>2.00</td>
<td>Finalised</td>
<td>Shelim Miah</td>
<td>31/10/2016</td>
</tr>
<tr>
<td>2.1</td>
<td>Review and update</td>
<td>Shelim Miah</td>
<td>29/09/2020</td>
</tr>
<tr>
<td>2.2</td>
<td>C.Lightfoot review</td>
<td>C.Lightfoot</td>
<td>03/12/2020</td>
</tr>
</tbody>
</table>

Authorisation:
Name / Position: Rachel Bence Chief Information Officer
Signature: Rachel Bence
Date: 15.02.2021
CONTENTS

1 POLICY STATEMENT ......................................................... 4

2 SCOPE ............................................................................. 4

3 POLICY DETAIL ............................................................... 4

4 MONITORING ..................................................................... 7

5 EXCEPTIONS ...................................................................... 7

6 REFERENCES ..................................................................... 7

7 APPENDIX A - DEFINITIONS ............................................ 7
1 Policy Statement

1.1 To ensure that anyone who has access to Queen Marys (QM) 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 QM.

1.2 The Policy aims to:
   - Outline the expectations of IT system and service users.
   - Ensure the security and protection of QM 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 QM IT services and systems. All users are required to behave in an appropriate manner that complies with all legal requirements and will not risk damaging QM’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 QM or by third parties on behalf of QM. These include, but are not limited to:

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

3.2 Failure to comply with the appropriate policies may lead to QM 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 QM and any legal action to which QM 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 QM, service providers or third parties.

3.5 Users must Comply with the Data Protection Policy, in particular the obligation to inform the QM 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 QM 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 QM systems for QM 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 QM owned equipment or software when requested to do so. N.B. personal data held on QM devices may be returned to the user where it is possible to do so. QM does NOT guarantee that personal data will be returned.

3.12 Users must return IT equipment to their line manager who shall return the items to IT Services when their employment contract is completed, suspended or terminated.

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

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

3.15 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 QM policies or business interests
   - Likely to bring QM into disrepute

3.16 Users must not use QM IT services in such a way as to risk or cause loss of damage to, or breach confidentiality of data or systems.
3.17 Users must not use IT services in a way that risks bringing QM into disrepute including associating QM with external facilities or bodies by association.

3.18 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.

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

3.20 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 QM.

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

3.22 Users must not connect any unauthorised device to Queen Mary’s network or information systems.

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

3.24 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 Monitoring

4.1 IT Services may request checks to be carried out as part of internal audits, any findings will reported to the IT Lead Team (ITLT) for any corrective actions to be issued.

4.2 Where non-compliance is identified and the corrective actions have not been implemented, ITS will take appropriate action, which may result in escalation to senior management.

5 Exceptions

5.1 Where an exception to this policy is required, the matter should firstly be referred to the ITLT to assess the exception.

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

5.3 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.

6 References

- SOP DG29 – Acceptable Use of IT
- DG05 Information Security Incident Reporting Policy
- Information Security Policy
- Student Contract and Acceptable Behaviour

7 Appendix A - Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>BYOD</td>
<td>Bring Your Own Device refers to users using their own device (which is not owned or provided to you by QM) to access and store QM information, whether at the place of work or remotely, typically connecting to the QM’s Wireless Service.</td>
</tr>
<tr>
<td>Data Controller</td>
<td>The Data Controller is a person, group or organisation (in this case QM) who determines the purposes for which and the manner in which any personal</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User</td>
<td>A member of staff, enrolled student, contractor, visitor, or another (any other) person authorised to access and use QM’s systems.</td>
</tr>
<tr>
<td>ITLT</td>
<td>IT Lead Team – Team of Senior Managers consisting of the Assistant Directors of IT, Faculty Relationship Managers and Chaired by the IT Director.</td>
</tr>
<tr>
<td>ITSB</td>
<td>IT Strategy Board – Team of Executive Managers consisting of Vice Principals and the IT Director, who oversee the delivery of the IT Strategy.</td>
</tr>
<tr>
<td>Account Sponsor</td>
<td>Can be a line manager or person of authority that is responsible and accountable for an IT Account that has been issued.</td>
</tr>
</tbody>
</table>