IT Services Policy

ITP03 - Bring Your Own Device (BYOD) Policy

Prepared by: < Shelim Miah>
Version: 1.3

Description & Target Audience: This document describes statutory use relating to using your own device to access Queen Mary University systems and services. This document is aimed at all Staff & Students within Queen Mary University of London.			
Effective Date:	**26/10/2016**	Review Date:	**26/10/2017**

Reviewers:	**Craig Walker, IT Service Desk Manager** **Ian Douglas, Head of IT Security** **Henrick Brogger, Head of Student & Staff Support Services** **Amit Patel, Head of Student & Staff Support Services** **Skender Osmani, Head of Client Devices & Audio Visual** **Martin Evans, Head of Data Centre Services** **Tavinder Jandu, Head of Network Infrastructure** **David Boakes, Assistant Director Student & Staff Services**
Policy Owner:	
Name/Position	David Boakes Assistant Director Student & Staff Services

Revision History			
Version	Description	Author	Date
0.1	Initial draft	Shelim Miah	14/11/14
0.2	Updated to reflect the comments from Aggi	Shelim Miah	14/11/14
0.3	Updates to reflect Ian Douglas' comments	Shelim Miah	17/11/14
0.4	Updates to section 4 reflect Martin Evans' comments	Shelim Miah	18/11/14
0.5	Updates on VDI to reflect Tavinder's comments	Shelim Miah	24/11/14
0.6	Updates to reflect Nigel Proctors comments	Shelim Miah	27/11/14
0.7	Update to formatting	Shelim Miah	27/11/14
0.8	Updates to capture Ian Dickson's comments	Shelim Miah	28/11/14
0.9	Updates from Tavinder Jandu second review	Tavinder Jandu	19/01/15
0.10	Updates from Shanaz Shahid	Shanaz Shahid	12/02/15
0.11	Updated from comments received from Sandra	Shelim Miah	09/03/15
0.12	Updates from David Boakes	Shelim Miah	17/04/15
0.13	Update from the IT Lead team	Shelim Miah	21/05/15
0.14	Update from David Boakes	Shelim Miah	25/05/15
0.15	Update From Johnathan O'Regan	David Boakes	27/07/15
1.0	Approved by HR document finalised	Shelim Miah	28/08/15
1.1	Feedback from Records & Information Compliance Manager	Shelim Miah	01/10/15
1.2	Exception for international use added	Shelim Miah	22/04/16
1.3	Annual Review – Template change only	Shelim Miah	25/10/16

Authorisation:	
Name / Position	**Mark Duff/ Interim Director of IT Services**
Signature	**M.Duff**
Date	**26/10/16**

CONTENTS

_Toc464645419

1 POLICY STATEMENT 4
2 SCOPE 4
3 POLICY DETAIL 5
4 BYOD GUIDELINES 7
5 ROLES & RESPONSIBILITIES 7
6 PROCESS AND PROCEDURES 8
7 MONITORING 8
8 EXCEPTIONS 8
9 REFERENCES 8
10 APPENDIX A 9
Appendix B Separate Document

1 Policy Statement

1.1 At Queen Mary University of London (QMUL) both staff and students make considerable use of mobile networking which provides access to information whilst on the move. This information is often accessed from a variety of mobile devices making it incumbent upon IT Services (ITS) to offer some level of support to users of these devices.

1.2 Mobile platforms such as laptops, PDAs and portable storage devices pose a particularly high security risk, primarily because they are vulnerable to theft and loss. Their material value is a secondary concern when compared to the potential cost of losing or compromising confidential, personal and/or sensitive data.

1.3 It is QMUL's intention to place minimal restriction on users' personal devices (BYOD) subject to QMUL meeting its legal obligations, for example the Data Protection Act and duty of care in how the data is managed and accessed.

1.4 This policy outlines what is expected from the user in order to use their BYOD for accessing, viewing, modifying and deleting QMUL held data and accessing IT systems. ITS does not currently offer a formal BYOD support service but understands that by offering the capability it has a responsibility to provide a basic level of support, subject to users following basic guidelines set out in this Policy.

1.5 The Policy aims to:

- Outline the expectations of users using BYOD
- Ensure the security and protection of QMUL data
- Implement controls to safeguard both users and support staff
- Outline roles & responsibilities
- Enhance Communications

2 Scope

2.1 This Policy is applicable to anyone using a non-QMUL-owned device for example laptops, PDA, smart phones, tablets and similar technologies, commonly known as a BYOD, to access QMUL data and/or IT services, this includes any visitors to the university.

2.2 All QMUL staff have access to a QMUL device either shared or personal, and should make every effort to use these devices as their primary work device. It is acknowledged that tablets and phones/PDAs etc. are used by staff and they therefore should be conscious of the security requirements in handling and storing QMUL data on their BYOD in accordance with SOP DG14 and DG15.

3 Policy Detail

3.1 It is the responsibility of the BYOD user to ensure they are aware and compliant with the Data Protection Act (1998) and the QMUL Data Protection Policy and understand the consequences of the loss of QMUL owned personal data.

3.2 All Students & Staff will be expected to agree and adhere to this Policy and comply with the QMUL Computer Use Regulations and all other IT and Information Security related Policies, if they wish to use BYOD.

3.3 Where the use of a BYOD becomes counterproductive, QMUL reserves the right to cease all BYOD activities for an individual/group or wider and where necessary may take action to prevent any further use.

3.4 ITS will support the setting up and connection to QMUL systems and accounts only where possible. Users have a responsibility to learn how to use and manage their device effectively.

3.5 QMUL takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding employee/student BYOD, or for any loss or damage resulting from support and advice provided.

3.6 Faults caused by user downloaded apps will not be rectified by ITS, instead the faulty or corrupted app will be requested to be removed by the user. Any app that causes security vulnerabilities unless removed from the device will be denied access to QMUL's systems/networks.

3.7 ITS will assist in changing passwords to QMUL services only. All personal sites, such as Facebook will have to be changed by the user.

3.8 IT Service Desk where possible, will provide guidance documentation that may help to rectify some software and virus issues, on a reasonable endeavours basis. ITS WILL NOT take responsibility to implement the remedial actions.

3.9 QMUL, as the Data Controller, remains responsible for all personal data, where the data has been obtained from QMUL systems and used or stored on any BYOD.

3.10 When using a BYOD for any purpose, users MUST maintain the security of QMUL's information at all times (which includes, but is not limited to; viewing, accessing, storing or otherwise processing). This applies to information held on QMUL systems.

3.11 Users will be required to assist and support QMUL in carrying out its legal and operational obligations, including co-operating with ITS Security should it be necessary to access or inspect QMUL data stored on BYOD.

3.12 QMUL reserves the right to monitor, investigate, refuse, prevent or withdraw access to users and/or any BYOD or software where it considers that there is unacceptable security, or other risks, to its staff, students, business, reputation, systems or infrastructure.

3.13 ITS may instruct users to update or install software that allows device management or enables access to or obtain information from their BYOD.

There is currently no remote access solution for students, access will be limited to systems that are web based. However Staff will be offered a remote access solution to help access QMUL applications.

3.14 This may require software to be installed on the BYOD and can be requested from ITS. Some applications due to licencing may not be available through the remote access solution and may need to be installed directly on to the device. It is the users' responsibility to familiarise themselves with their BYOD to protect information from being lost or stolen or accessed by third parties.

Information can be protected by using controls such as PIN/Password and passphrase locks on BYOD.

3.15 Information held on the BYOD that is deemed Highly Confidential or Confidential as per the SOP DG09 – Information Classification must be encrypted to the appropriate standard as outlined in the SOP Encryption and if this cannot be achieved must not be stored on the BYOD.

3.16 Any staff or student handling NHS patient data are bound by NHS standards and should not export data except where clear information sharing protocols have been set and appropriate ethics and Caldicott sign off secured.

3.17 Personal data as defined by the Data Protection Act (1998) and QMUL sensitive and confidential information may not be stored on any cloud services such as Dropbox, Google Drive without express approval from the Information Governance Group.

3.18 The storage and handling of personal, sensitive and confidential data held on the BYOD must comply with the SOP DG14 - Storage of Information and DG15 - Handling Information.

3.19 Portable storage devices (USB memory sticks and hard disks) that contain sensitive, confidential QMUL data and any personal identifiable data (PID) must always be encrypted. Many devices are supplied with proprietary encryption mechanisms which are easy to configure and use. Open source, cross-platform alternatives are available for devices that do not have built-in encryption.

3.20 There are suitable applications that are approved by QMUL, which offer suitable encryption and can be used for mobile storage devices. These are shown in Appendix B

3.21 In the event of the device being lost or stolen, this must be reported to ITS Security via the IT Service Desk to be managed in accordance with SOP DG27 – IT Security Incident Management.

3.22 In an event of a security incident, IT Security may decide that the lost or stolen device must be wiped in order to protect QMUL information. If such a decision is made, the device may be wiped by ITS Security or the user will be instructed to do this. This may result in the loss of personal data, such as photos and contacts for which QMUL will not be held responsible.

4 BYOD Guidelines

4.1 ITS will make reasonable endeavours to support users in connecting or using QMUL Systems, but may be unable to support those BYOD where basic good practice has not been followed such as:

a. Users should set bootup (BIOS) passwords for laptops and PINS for tablets, phones and PDA etc. Passwords that are set for all BYOD should conform to the password setup guidelines outlined in the QMUL Security Policies.
b. Users should set screen locks and automatic screen locks to ensure that BYOD lock automatically when not in use recommended; 1 min for phones, tablets and PDAs and 10 mins for laptops.
c. Users to ensure that all BYOD software/firmware must be kept up to date with the latest release for the device.
d. Users to ensure that any encryption facilities on the BYOD is activated if available.
e. Ensure a reputable antivirus protection is installed on the BYOD where applicable.
f. Users should activate or install any tracking and wiping services, for example Apple's 'Find My iPhone'.
g. Users must remove any QMUL information stored on the BYOD if this is no longer required. This includes deleting copies of attachments to emails, such as documents, spreadsheets and data sets.
h. Users must remove all QMUL information from BYOD and return it to the manufacturer's settings before the device is sold, exchanged or disposed of.
i. Any BYOD found to have the manufacturer's security mechanisms circumvented, such as 'jailbreak' will not be supported and ITS have the right to deny access to reduce the risk to the QMUL network.

5 Roles & Responsibilities

5.1 The user is responsible for the BYOD and should not leave it unattended. The user is responsible for any unauthorised access or misuse that may occur at the hands of a 3rd party with or without the knowledge of the user.

5.2 It is the responsibility of the user to enable password and PIN protection on the BYOD.

5.3 The user is responsible for enabling and configuring any encryption facilities and storing passwords in a safe and secure manner. The user will also be responsible for changing the password immediately on discovery that the password may have been compromised and to inform IT Security via the IT Service Desk immediately.

5.4 The responsibility for back-up and recovery is with the user.

5.5 It is the responsibility of the user to familiarise themselves with the QMUL Standard Operating Procedures on handling, storing and transferring data.

6 Process and Procedures

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

7 Monitoring

7.1 It is mandatory for anyone using a BYOD to comply with the IT Policies and any associated procedure. Where non-compliance is identified, ITS will take appropriate action, which may result in the BYOD being barred from the QMUL network.

7.2 Checks may be made by the IT support whilst delivering support to users. IT support may report their findings to IT Security of any breach of its Policies and may instruct the user to take corrective actions.

7.3 The Head of Student and Staff Support Services, in conjunction with the Risk & Governance Manager, is responsible for the monitoring, revision and updating of this document.

8 Exceptions

8.1 Exemptions may be provided to aspects of this policy where there is a conflict with the law in the country the BYOD is being used. In such circumstances Users must take extra precautions to guard against the vulnerability that is being exposed, for example not storing sensitive or transferring information across the network.

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

8.3 The ITLT will then make a decision or refer this to the IT Strategy Implementation Board (ITSIB) for guidance.

9 References

- BYOD Nottingham Trent University
- Mobile Device Policy – Kings College
- QMUL ARCS Webpage

10 Appendix A

10.1 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.
ITSIB	IT Strategy Implementation Board – Team of Executive Managers consisting of Vice Principals and the IT Director, who oversee the delivery of the IT Strategy.