IT Services Policy / Policy Document

ITP07 - Self-Managed Device

Prepared by: Kaptan Miah and Sarah Lai
Version: 1.5

Effective Date : 23/03/2022	**Next Review Date : 23/03/2023**

Reviewer's name : As per approvers and distributions list.
Policy Owner/s: Tom King and Henrik Brogger
Name / Position : **Tom King – ITS Assistant Director of Research** **Henrik Brogger – ITS Head of Service Delivery**

Distribution			
Name	**Title**	**Date of Issue**	**Version**
Anne Parry	Faculty Director of Operations S&E	17 Jan 22	1.1
Jonathan Croft	IT Manager FMD	17 Jan 22	1.1
Paul Smallcombe	Records & Information Compliance Manager	17 Jan 22	1.1
Matthew Trump	Information Security Manager	17 Jan 22	1.1
Robert Bennett	Faculty Director of Operations FMD	17 Jan 22	1.1
Marie Gallagher	Faculty Director of Operations H&SS	17 Jan 22	1.1

Authorisation
Name / Position : Rachel Bence
Signature : Rachel Bence
Date : 21 Mar 2022

1. Contents

2. Policy Statement

This policy has been formulated to cover requests for self or un-managed devices (henceforth self-managed). These are devices that are not pre-loaded with an image or similar software configuration by IT Services, allowing the recipient full administrative access to the device software. The document objective is to ensure that staff understand and accept their responsibilities and obligations in owning a self-managed device.

All self-managed devices must be used in accordance with the Information Governance policies which can be found here

3. Business Case

Users requesting a self-managed device are required to submit a brief business case outlining the rationale for the request. The business case needs to be accompanied by written approval from the line manager/PhD supervisor.

The rationale should outline why the exception should be made for a self-managed device. Please note, simply stating the inconvenience of contacting the IT ServiceDesk for support will not be sufficient and the request will be rejected. The request must be submitted to the IT ServiceDesk via email or using the self-service portal with a business case. See section 13.2 (email signature) for submitting an electronic request.

The request will then be reviewed by the ITS Research Consultants and, if appropriate, passed to the relevant Faculty Directors of Operations for their review and approval.

4. Faculty Approval

Faculty Directors of Operations should review the business case with the understanding that the self-managed devices introduce an increased risk to the organisation and the cost to support these devices is inherently higher than that of managed devices.

Unmanaged devices pose a greater risk to QM than managed devices, the approving line manager and user of the device will be responsible for the associated risk.

Approval should only be granted if it otherwise stops the timely and cost-effective delivery of research.

The ITS Research Facilitation team can be consulted for further advice.

5. Data Management Plan and Data Storage

The end-user (primary user on a day-to-day basis) of the self-managed device is primarily responsible for managing data on the device as defined by QMUL’s IT Policy and SOPs (Standard Operating Procedures). It is beyond the scope of this document to go into details about individual SOPs, but all SOPs along with IT policy are available for inspection at:
https://www.its.qmul.ac.uk/governance/policies/

The end user of the self-managed device is advised to review these documents (SOPs) to understand their responsibilities before accepting the self-managed device.

The end-user of a self-managed device is responsible for the backup of the data stored on the laptop/desktop.

As per our draft data storage approach and supporting matrix, **all** data of value to the institution whether related to teaching, administration or research should only be held **temporarily** on a self-managed device.

Therefore, the end user inherits the responsibility of selecting and using an appropriate storage platform for backing up their data according to its information classification. Users are advised to continue to use their usual storage platform with a self-managed device such as *QMUL's OneDrive for Business, Apocrita (ITS Research Storage) and Data Safe Haven* (NHS/FMD). If you need further guidance on these storage platforms, contact the IT Research Facilitator to assist you in identifying a suitable storage platform for your data.

The end-user of the self-managed device must ensure that all the data is stored according to QMUL's Information Classification (SOP DG09) and appropriate controls are in place as defined by Information Classification SOP. Furthermore, researchers are reminded to ensure that they adhere to any specific condition set by the data owner for processing and storing data for individual research projects (i.e as defined by DMP/research protocol).

In all cases, personal identifiable information (PII) should not be held on a self-managed device without a detailed assessment of the risks involved. This can be undertaken by the ITS Research Facilitators, ITS Information Security team and/or Barts Cancer Centre IT staff.

6. Software licensing

Users will be responsible for ensuring that all software installed on a self-managed device is correctly licensed.

In some cases, due to both technical and licensing constraints, although software may be available free of charge on a managed device, this may not be available on a self-managed device. Therefore, end-users should budget for software purchases prior to submission of the business case.

On occasion, IT Services are obliged to carry out licensing audits either at the request of software vendors or senior committees of the University. Where possible, IT Services will install software to automate this activity, but end users may be required to carry out this task.

7. Support

7.1 Security controls

By taking ownership of the self-managed device, you are expected to implement security controls equivalent to that of ITS managed service platforms. These are detailed in the Information Security policies available on our website, but the following is a summary of the controls you should be actively applying and monitoring.

7.1.1 Operating System

IT Services will only permit you to use an operating system which is currently supported or for which security updates can continue to be obtained.

7.1.2 User access controls

- Implement strong passwords on all local operating system accounts – equivalent to and better than the current ITS specification. Please find information here for setting password.
- Separate user and local administrator accounts where possible and rename OS built-in accounts like ‘Administrator’, ‘Guest’ and change their passwords/disable accounts.
- Do not use an account with administrative privileges for normal working.
- Do not provide access to non-QMUL users.
- The BIOS/UEFI should be locked from unauthorised access with a strong password.

7.1.3 Security Updates

The end-user is primarily responsible for ensuring that relevant **security patches are applied** as soon as possible to reduce the risk associated with having a self-managed device connecting to the University’s network. This should include keeping all software up to date with relevant security patches (e.g. routinely applying the latest OS security updates/vulnerability, updating antivirus definition files).

7.1.4 Security software

The end user is explicitly forbidden from uninstalling and disabling any software came pre-installed with a self-managed device that is used to enhance the security of the device or is required for IT compliance purposes.

IT Services makes available Endpoint Threat Detection software e.g. virus scanners for installation on devices and users should ensure that these are installed and running.

IT Services may install additional device management software to locate and disable self-managed devices in the event of theft, you are expected to ensure that this software is active.

Should any security software be found missing it will be re-installed immediately without seeking confirmation.

7.1.5 Firewall

The end user is expected to install and maintain a host firewall in operation on the device. If as a part of their work, they need to enable incoming access, they should only open the appropriate ports and scope access to the smallest possible range of clients. Where possible, they should only permit encrypted protocols.

Where possible, Endpoint security software should still permit inspection of this traffic.

7.1.6 Base applications

Subject to availability on the operating system

1) MS Office365 and Teams
2) Lansweeper – configured to upload regular audit reports whether on or off the QMUL network
3) Anti-virus or Endpoint security tools configured to update daily and other essential protective settings
4) Fortinet VPN – configured with appropriate QMUL self-managed VPN settings

We retain the right to add/remove further base applications without seeking confirmation.

7.2 Getting Help

IT Services' ambition is to provide a comprehensive and secure managed service. We can only offer limited support for self-managed devices. Therefore, support will be on a *best endeavours'* basis. Further and additional support may be available on a chargeable basis.

The IT Service Desk will only accept requests to support application software which is licensed centrally by the University and not software that have been purchased and obtained by the user directly.

Should the software installation on the device become corrupted or otherwise unworkable, IT Services offers to reinstall the basic operating system and the base software initially provided before the device was handed to the user. Similarly, if a system upgrade is desired by the user, IT Services will install the new operating system and any base software as deemed necessary by IT Services only Please note IT Services does not accept any responsibility or liability for the state of the device before a reinstallation, nor for any data, software or configuration added after the device was initially handed to the user.
Please also note that all IT devices should be purchased through ITS as per the IT Device Policy found under policies here https://www.its.qmul.ac.uk/governance/policies/

8. Incident Reporting

Any security–related, theft or data loss incidents must be raised immediately with the ITS Service Desk. Live Chat: https://www.its.qmul.ac.uk/. Phone: +44 20 7882 8888 or servicedesk@qmul.ac.uk

9. Audit and review

There is an expectation for IT Services to request validation that users are meeting the security controls of self-managed devices with suitable warning. This could be undertaken by Campus Support, Research, Networks, Barts Cancer Centre IT staff, Information Security or the delegates and sub-contractors.

IT staff may remedy any discrepancies or advise users on the best practice. As with all agreed university policies, **wilful contravention of the IT policy can be considered a disciplinary offence** that can be reported to senior staff within the School, Institute or Department and/or lead to the reinstallation and/or removal of the device.
Please find link to policies below:
https://www.qmul.ac.uk/careers/media/careers/docs/Code-of-Student-Discipline.pdf
https://hr.qmul.ac.uk/procedures/policies/conduct/

10. Exceptions

This policy is effective from dates as per stated at the beginning of the policy.
Unmanaged devices issued prior to this date may not have all the base applications as stated in 8.1.6 installed.
However, compliance to all sections of this Policy still apply and IT Services will upgrade these Unmanaged devices as part of the operational activities when possible.

In the event of further exceptions that are not addressed by this Policy, the matter will be first referred to the appropriate Faculty Relationship Manager for advice and guidance.

11. References

DG09 – Information Classification
DG14 – Storage of Information

- All users of services provided by QMUL ITS must abide by the ITS Policies and Standard Operating Procedures (SOPs) that can be found at: http://www.its.qmul.ac.uk/governance/policies/index.html.

- Overarching Policies can be found on the QMUL Academic Registry and Council Secretariat (ARCS) Policy zone page under "Information and IT-related policies and procedures" at: http://www.arcs.qmul.ac.uk/policy/index.html.

12. Appendices

Appendix A: Definitions

Term	Meaning
Self-managed ,unmanaged	Both terms are used interchangeably. This means the end-user has the administrative privilege (root privilege) to install, remove and modify the software on the device and does not have system updates and security patches applied centrally by IT Services. It also means the end-user has extended responsibilities in regard to maintaining the device, e.g. keeping software updated to minimise security risks.
Owner, End-user, You/your	All these terms are used interchangeably to mean the end-user/owner. The principal user who requested to have the self-managed device (i.e., named user of the device associated with ITS' asset tag)
DMP (Data Management Plan)	Data Management Plan used widely by various funding bodies EPSRC / UKRI.
OdfB (OneDrive for Business)	QM's SharePoint and OneDrive for Business (data storage platform) https://www.its.qmul.ac.uk/services/service-catalogue-items/communication-and-collaboration/email-and-collaboration-services/file-sharing/
Data Safe Haven	Sensitive patient-identifiable data storage platform (FMD/NHS) in our case operated on a chargeable basis by the Barts Cancer Centre.

Apocrita	ITS Research storage platform attached to the Apocrita HPC service.

Appendix B: Email confirmation of acceptance

Add the text below to your email request for a self-managed device. By sending the text below (*Italic*) you accept your responsibility and obligations outlined on this policy documents and other reference documents therein.

I acknowledge and agree to comply with the proper use of the self-managed device to conduct University work as detailed in this policy document and other documents listed in the reference section of this document and agree to the terms and conditions therein.
I will engage in any audit or review of my self-managed device and understand that failure to show compliance with this policy may lead to my right to have an unmanaged device being revoked.

Revision History			
Version	**Description**	**Updated by**	**Date**
0.1	Initial version	Kaptan Miah	18 Nov 21
0.2	Requested to reference Information/Data Governance Policy (DG14)	Henrik Brogger	19 Nov 21
0.3	Security controls	Tom King	23 Nov 21
0.4	Support and licensing	Alem Million	25 Nov 21
0.5	DMP/ Research data	Kaptan Miah	25 Nov 21
0.6	Exceptions – raised by SM	Sarah Lai	03 Dec 21
0.7	Additional security information – raised by AP Insert links to information governance suite for further cyber/info governance information	Matthew Trump & Rhianne Short	11 Jan 22
1.0	Finalise draft and amendments made	Sarah Lai and Henrik Brogger	17 Jan 22
1.1	Section 7.12 'Local' Administrator – raised by IA Update approval process 12.3 – raised by TK	Sarah Lai	3 Feb 22
1.2	Update appendices section 12 and insert audit process	Sarah Lai and Henrik Brogger	9 Feb 22
1.3	Accept and approve feedback from LT and InfoSec. AH (CISO) to approve	Henrik Brogger and Tom King	18 Feb 22
1.4	Document Finalised and Approved	ITLT	23 Mar 22
1.4a	Updates to section 3, 7.2, Appendix B	Henrik Brogger	23 May 22
1.5	Finalised and Re-published	Shelim Miah	25 May 22

Approvals			
Approver	**Title**	**Date of Issue**	**Version**
Tom King	AD ITS Research (Interim FRM)	17 Jan 22	1.1
Skender Osmani	Head of Client Devices	17 Jan 22	1.1
Henrik Brogger	Head of Service Delivery	17 Jan 22	1.1
Kaptan Miah	Research Facilitator – Digital Humanities	17 Jan 22	1.1
Alem Million	Research Facilitator – Life Sciences	17 Jan 22	1.1
Shelim Miah	Risk and Governance Manager	17 Jan 22	1.1
Rhianne Short	InfoSec – Policies Standards & Awareness	17 Jan 22	1.1
SMT	Members of the Senior Management Team	25 Jan 22	1.1
LT	ITS Lead Team	11 Feb 22	1.2
Matthew Trump	Information Security Manager	22 Feb 22	1.4
Fatuma Mahad	ITS Office of the CIOS (Rep InfoSec)	11 Mar 22	1.4