IT Services Policy

DG07 – Procuring IT Hardware & Software

Prepared by: <Shelim Miah>
Version: 2.1
Effective Date: 02/02/2023  
Review Date: 02/02/2024

Reviewers:  
Rhianne Short, Information Security Manager  
Shelim Miah, Risk & Governance Manager

Policy Owner:  
Name/Position: Rachel Bence, Chief information Officer

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>William Mordaunt</td>
<td>19/04/2010</td>
</tr>
<tr>
<td>1.1</td>
<td>Transferred onto a Policy Template</td>
<td>Shelim Miah</td>
<td>22/03/2016</td>
</tr>
<tr>
<td>2.0</td>
<td>Finalised</td>
<td>Shelim Miah</td>
<td>05/02/2019</td>
</tr>
<tr>
<td>2.1</td>
<td>Review</td>
<td>Shelim Miah</td>
<td>02/02/2023</td>
</tr>
</tbody>
</table>

Authorisation:

<table>
<thead>
<tr>
<th>Name / Position</th>
<th>IT Lead Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td>IT Lead Team</td>
</tr>
<tr>
<td>Date</td>
<td>02.02.23</td>
</tr>
</tbody>
</table>
CONTENTS

1 POLICY STATEMENT...........................................................................................................4
2 SCOPE....................................................................................................................................4
3 POLICY DETAIL.....................................................................................................................4
4 PROCESS AND PROCEDURES.............................................................................................6
5 ROLES & RESPONSIBILITY .................................................................................................6
6 MONITORING........................................................................................................................6
7 EXCEPTIONS ..........................................................................................................................6
8 REFERENCES ..........................................................................................................................6
9 APPENDIX A - DEFINITIONS ..............................................................................................7
10 APPENDIX B – USEFUL PROCUREMENT LINKS ...............................................................8
1 Policy Statement

1.1 This document ensures that IT hardware and software procurement is carried out in accordance with QMUL procurement policy and industry best practice.

1.2 The Policy aims to:

- Outline the expectations of all staff purchasing IT hardware & software.
- Ensure a consistent approach for all purchases.
- Comply with the QMUL Procurement policy
- Outline roles & responsibilities.
- Enhance Communications.

2 Scope

2.1 This policy applies to all IT hardware and software procurement, including open source software. This applies to all staff purchasing or requesting the purchase of IT hardware and software.

3 Policy Detail

3.1 All procurement of IT hardware and software must adhere to the QMUL procurement policies and guidelines.

3.2 Purchases are to be made using the QMUL framework agreements where appropriate. Where exceptions are necessary, such purchases must conform to the relevant procurement procedures.

3.3 Procurement of IT hardware and software shall correspond to the relevant QMUL standard specifications, where these exist the relevant Contract Supplier should be used. Where a standard specification is not applicable, a statement of business requirement must be provided by the procuring department and a formal request for change generated. Refer to DG25 – Configuration Management and Change Control.

3.4 All procured hardware and software shall be fully compatible with the QMUL network environment as necessary and evaluated as such under the QMUL change management process.

3.5 Open source software are to be approved by IT Services before being installed on to central IT services. Installation on local devices (self-managed) must be done so with the consultation of local school administrators.

3.6 All Open source and procurement of software assets must satisfy all relevant legislative, intellectual property and regulatory requirements and not expose QMUL to any risk on these terms.

3.7 Proposed procurements shall be subject to a risk assessment to ensure that they do not introduce unacceptable risk. A statement of business requirements, including a specification of security controls are to be provided with the proposed procurement.

3.8 When a proposed purchase includes the option of an extended warranty at additional cost, whole life costing shall be taken into account and the advice of the Procurement department sought as required.
3.9 Delivery of new IT assets shall be only to standard QMUL addresses or authorised exceptions to such a list of approved addresses, as maintained by ITS Business Support team or equivalent, and shall be accepted only by authorised QMUL staff or authorised delegates.

3.10 Release and installation procedures for IT assets shall conform to QMUL testing, release, and configuration management controls as set out in DG08 - Implementing IT Systems.

3.11 All procured IT hardware and software shall be added to the relevant asset and configuration management databases and appropriate physical or electronic labelling carried out. Entries in asset and configuration databases shall identify ownership of the asset and categorise the asset in terms of business value, security classification and information security risk assessment and contain such information as may be required for health and safety and insurance purposes.

3.12 Asset and configuration management database entries for new IT assets shall include all information required to satisfy the requirements of the QM Business Continuity policy.

3.13 All IT hardware asset purchases shall be recorded in such a way as to enable effective operational lifecycle management and satisfy the terms of DG10 - Disposal of IT Equipment.

3.14 Lost, damaged or stolen hardware or software assets shall be reported in accordance with DG27 - IT Security Incident Management.
4 Process and Procedures

4.1 The associated processes and guidance documents can be found by visiting the [QMUL Procurement webpage](https://www.qmul.ac.uk/).

5 Roles & Responsibility

5.1 The Risk and Governance Manager will be responsible for initiating the review cycle for the policy, process document owner to carry out the review. The Document owner will assess and incorporate any comments or feedback received.

5.2 Once the document has been updated, the Risk and Governance Manager will take the document to the appropriate board for approval. All approved documentation are to be stored in a central repository and uploaded to the web where applicable.

6 Monitoring

6.1 It is mandatory for anyone procuring IT hardware and or software to comply with this IT policy and any associated procedure. Where non-compliance is identified, ITS will take appropriate action.

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

6.3 The Assistant Director of IT Operations, in conjunction with the Risk & Governance Manager, is responsible for the monitoring, revision and updating of this policy.

7 Exceptions

7.1 In the event of an exception that is not addressed by this Policy. The matter will be firstly referred to the ITLT for a decision.

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

8 References

- SOP DG01 – Information Risk Assessments
- SOP DG02 – Business Continuity
- SOP DG08 – Implementing IT Systems
- SOP DG10 – Disposal of IT Equipment
- SOP DG25 – Configuration Management and Change Control
- SOP DG27 – IT Security Incident Management
- QMUL’s published Procurement Policies
- Business Support Services internal BSS SOPs
- SOP DG07 – Procuring IT Hardware & Software
- [Capital Expenditure Policy](https://www.qmul.ac.uk/)
- [Financial Regulations](https://www.qmul.ac.uk/) [PDF 659KB]
## Appendix A - Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Asset</td>
<td>Assets include all elements of software and hardware that are found in the IT environment.</td>
</tr>
<tr>
<td>Risk</td>
<td>A Risk can be anything (an action, event or set of circumstances) that can adversely or beneficially affect QMUL’s ability to achieve its current or future objectives.</td>
</tr>
<tr>
<td>SOP</td>
<td>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.</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 QMUL’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>
</tbody>
</table>
## Appendix B – Useful Procurement Links

<table>
<thead>
<tr>
<th></th>
<th>Link to procurement intranet Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>To set up new suppliers</td>
<td><a href="http://qm-web.finance.qmul.ac.uk/purchasing/new-supplier-request/">http://qm-web.finance.qmul.ac.uk/purchasing/new-supplier-request/</a></td>
</tr>
</tbody>
</table>