IT Services Policy

DG17 – IT User Account Management

Previously Known as: User Account Registration SOP
Prepared by: <Shelim Miah>
Version: 2.3
Description & Target Audience: This document outlines when an IT Account can be issued and when it may be disabled, it also outlines the expectations of those who have been issued an account. This document is aimed at all Staff & Students who are issued an IT Account within Queen Mary’s University.

Effective Date: 23/01/2018 Status: 23/01/2021

Reviewers: Kathy Whelan, IT Service Desk Manager
Ian Douglas, Chief Information Security Officer
Henrik Brogger, Head Service Delivery
Amit Patel, Head of Service Management
Martin Evans, Head of Data Centre Services
Jason Bunning, Head of Student Systems
David Boakes, Assistant Director IT Operations

Policy Owner: Rhys Davies, 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>1.4</td>
<td>Initial draft</td>
<td>Shelim Miah</td>
<td>01/03/16</td>
</tr>
<tr>
<td>1.5</td>
<td>Comments received from Ian.</td>
<td>Shelim Miah</td>
<td>04/03/16</td>
</tr>
<tr>
<td>1.6</td>
<td>Comments received from Henrik</td>
<td>Shelim Miah</td>
<td>08/03/16</td>
</tr>
<tr>
<td>1.7</td>
<td>Further amendments on best practice clause</td>
<td>Shelim Miah</td>
<td>11/03/16</td>
</tr>
<tr>
<td>1.8</td>
<td>Review with AD Student &amp; Staff Services</td>
<td>Shelim Miah</td>
<td>15/06/16</td>
</tr>
<tr>
<td>1.9</td>
<td>Draft finalised</td>
<td>Shelim Miah</td>
<td>16/06/16</td>
</tr>
<tr>
<td>1.10</td>
<td>ITLT Feedback – add disclaimer</td>
<td>Shelim Miah</td>
<td>23/08/16</td>
</tr>
<tr>
<td>1.11</td>
<td>Feedback from HoS Service Management</td>
<td>Shelim Miah</td>
<td>08/09/16</td>
</tr>
<tr>
<td>1.12</td>
<td>Updated Disclaimer section</td>
<td>Shelim Miah</td>
<td>16/09/16</td>
</tr>
<tr>
<td>2.00</td>
<td>Finalised</td>
<td>Shelim Miah</td>
<td>21/09/16</td>
</tr>
<tr>
<td>2.1</td>
<td>Annual Review,</td>
<td>Shelim Miah</td>
<td>23/11/17</td>
</tr>
<tr>
<td>2.2</td>
<td>Updates based on feedback received</td>
<td>Shelim Miah</td>
<td>10/01/18</td>
</tr>
<tr>
<td>2.3</td>
<td>Finalised</td>
<td>Shelim Miah</td>
<td>15/01/18</td>
</tr>
</tbody>
</table>

Authorisation:

Name / Position: Rhys Davies, Chief Information Officer
Signature: Rhys Davies

Date:
CONTENTS

1 POLICY STATEMENT ........................................................................................................4
2 SCOPE ..................................................................................................................................4
3 ACCOUNT CREATION ........................................................................................................4
   Students .............................................................................................................................4
   Staff .....................................................................................................................................5
4 MANAGING ACCOUNTS ...................................................................................................5
5 ACCESS PRIVILEGES .......................................................................................................5
6 DISABLING ACCOUNTS ....................................................................................................6
7 GUEST ACCOUNTS ............................................................................................................7
8 PROCESS AND PROCEDURES ........................................................................................8
9 MONITORING ....................................................................................................................8
10 EXCEPTIONS ...................................................................................................................8
11 REFERENCES ....................................................................................................................8
12 APPENDIX A ....................................................................................................................9
   Definitions .......................................................................................................................9
1 Policy Statement

1.1 To ensure that IT user registration and account creation is carried out in accordance with QMUL policy and industry best practice and to ensure authorised users are given the appropriate access when required.

1.2 The Policy aims to:

- Outline the expectations of IT account holders.
- 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 all IT user accounts, including e-mail and Internet services. Users, either studying or working at QMUL, or those who wish to register for access to QMUL IT services.

3 Account Creation

3.1 By using QMUL IT services all users are understood to agree, that they will comply with QMUL’s ‘Conditions of Access to Computing Facilities Agreement’. New users should be notified of the acceptable uses of QMUL computing systems before they are given access.

3.2 QMUL IT user accounts are issued to new users by IT Services (ITS) for both Students e.g. AB12345 and Staff e.g. ABC123. In certain circumstances, students may be granted both a student and staff account and staff may also have both a staff and student account.

3.3 No access to QMUL information systems will be granted until the registration, application and appropriate approval procedures have been completed.

3.4 All new user account requests are to be processed by the relevant QMUL IT service provider in accordance with the QMUL IT Policies, Regulations, Terms and Conditions.

3.5 ITS will only create accounts that are requested via an authoritative source.

Students

3.6 New user accounts for students are to be controlled by a formal process with requests generated by Registry or appropriate departmental Heads of Department or IT representatives.

3.7 Students enrolling at the start of term only, may have their credentials sent to them before they are enrolled, provided measures are in place to protect against unauthorised access.
3.8 Bulk requests for new user accounts, e.g. those for new students at the start of the academic year, are to be processed automatically and granted pre-defined levels of access to services.

Staff

3.9 All staff account requests are to be made to ITS by-line managers or those with the equivalent authority to do so.

3.10 Staff user access will be set up after processing of the relevant application(s) but full standard access will not be made available in advance of the individual’s QMUL employment or supplier contract date.

4 Managing Accounts

4.1 An Individual may have one or more user accounts i.e. a student may also have a staff account.

4.2 All efforts must be made to ensure Individuals who have multiple statuses within QMUL (e.g. student and staff) are given one account and assigned multiple roles where possible. Separate accounts may only be issued where the former is not technically possible. In this instance users must use the account for the purpose they were provided for.

4.3 No account must be shared with any other person for any reason. ITS will monitor usage and activities from time to time.

4.4 All account holders must ensure that their passwords are kept safe and secure at all times and are subject to the DG18 – Password Management Policy.

4.5 All account holders are subject to the ‘Acceptable Use Policy’. All IT polices are available on the ITS Website

4.6 The name and contact details of staff joining QMUL must be added to the staff directory and removed when they leave by the local Departmental Directory Administrator.

5 Access Privileges

5.1 Requests for access to information systems (Agresso, SITS) will require authorisation from the relevant system owner/data custodian. This may be implicit via the Service Desk or via local standard process/procedures and in writing.

5.2 Where no system owner/data custodian is identified, someone suitably senior from the school or area where the data resides needs to approve the request.

5.3 New user account requests, when approved, will provide standard levels of access to QMUL information services. Enhanced access is to be requested via the Service Desk. Access levels will
be granted appropriate to meet business needs only and meet the requirements of the IT Policies i.e. minimum level of access.

5.4 Special privileges, including system administration and programming rights, will be granted only after authorisation from the system owner and is to be requested via the Service Desk.

5.5 User access rights (normal and enhanced) and/or privileges are to be reviewed and modified as appropriate, it is the line manager’s/supervisors responsibility to inform ITS when moving from one role to another within QMUL. The line manager/supervisor is to ensure that the level of access is appropriate to the new function only unless it is a conscious decision to maintain their current privileges.

5.6 Where possible ITS and other appropriate departments should be given 2 weeks’ notice by line managers regarding changes to roles and functions that may affect their privileges.

5.7 ITS will deny access or disable an account where it considers a security risk or a violation of any IT Policy.

6 Disabling Accounts

6.1 HR/School Managers/School Admins and Line Managers must notify ITS and any other relevant system owning departments promptly of any contract terminations and/or student registration expiries. Access rights to information and information systems/IT accounts/Emails will be disabled. Where verbal requests have been made a follow up with written confirmation will be required.

6.2 When a student graduates and not returning for further study, their account is disabled, all information pertaining to that account will be deleted in accordance to the QMUL retention schedule.

6.3 In the case of staff, the account is disabled on the last day of the employment and information deleted in accordance with the retention schedule.

6.4 Access rights to information and information systems may be reduced, removed or extended, prior to termination depending on a risk assessment. This may include factors such as: whether termination was initiated by the user or QMUL, the reason for the termination, the current responsibilities of the user and the value and sensitivity of data that they access.

6.5 Users who wish to be contactable following the closure of their account must ensure that they record an automatic reply or forwarding prior to the closure of their email account. The automatic reply/forward will continue to operate until the account is deleted.

6.6 The user is responsible for ensuring any personal data held in their IT account(s) is transferred and/or deleted off the IT network before the account is disabled.

6.7 Where an account extension is required it is the responsibility of the School/Departmental Manager or equivalent to detail the reason for the account extension, the length required, and must be requested before the account is disabled. The School/Departmental Manager or equivalent will remain responsible and accountable for the account extension.
7 Guest Accounts

7.1 Guest Account(s) are subject to the same QMUL Policies, Regulations, terms and conditions as any other IT user at QMUL.

7.2 For the purpose of this document the term ‘Guest Account’ includes; visitor and temp accounts.

7.3 Before any Guest Account(s) are issued, the reason for the Guest Account must be outlined along with a form of picture identification of the individual account holder(s).

7.4 Guest Accounts must be created with an expiry date and a named member of staff (sponsor) made responsible and accountable for these accounts.

7.5 It is the account sponsors responsibility to ensure the user of the Guest Account is fully aware and compliant with QMUL Policies, Regulations, terms and conditions.

7.6 Guest Accounts must be tied to an individual and must not be shared or inherited, the access privileges are to be restricted to the requirements of their role.

7.7 Guest accounts may not have access to data or systems classified as ‘Restricted’ or higher.

7.8 If the expiry date of an account has not been reached and the account is no longer required, ITS must be informed immediately by the account sponsor and ITS will disable the account.
8 Process and Procedures

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

9 Monitoring

9.1 It is mandatory for anyone using an IT Account to comply with the IT Policies and any associated procedures. Where non-compliance is identified, ITS will take appropriate action, which could result in the IT Account and associated information system access being disabled and where appropriate may lead to disciplinary actions.

9.2 Where breaches of IT Security and or Policies are suspected or detected they are to be reported to IT Security via the Service Desk.

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

10 Exceptions

10.1 In the event of an exception that is 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.

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

11 References

- SOP DG17 - User Registration
## Appendix A

### 12.1 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 QMUL) to access and store QMUL information, whether at the place of work or remotely, typically connecting to the QMUL’s Wireless Service.</td>
</tr>
<tr>
<td>Data Controller</td>
<td>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.</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>
<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>