Queen Mary
University of London

IT Services Policy

DG17 – IT User Account Management

Prepared by: < Shelim Miah>
Version: 2.0

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 Marys University.			
Effective Date:	**23rd Sept 2016**	Review Date:	**23rd Sept 2017**

Reviewers:	**Kathy Whelan, 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** **Martin Evans, Head of Data Centre Services** **Jason Bunning, Head of Student Systems** **David Boakes, Assistant Director Student & Staff Services**
Policy Owner:	
Name/Position	Mark Duff, Interim Director of IT Services

Revision History

Version	Description	Author	Date
1.4	Initial draft	Shelim Miah	01/03/16
1.5	Comments received from Ian.	Shelim Miah	04/03/16
1.6	Comments received from Henrik	Shelim Miah	08/03/16
1.7	Further amendments on best practice clause	Shelim Miah	11/03/16
1.8	Review with AD Student & Staff Services	Shelim Miah	15/06/16
1.9	Draft finalised	Shelim Miah	16/06/16
1.10	ITLT Feedback – add disclaimer	Shelim Miah	23/08/16
1.11	Feedback from HoS Service Management	Shelim Miah	08/09/16
1.12	Updated Disclaimer section	Shelim Miah	16/09/16
2.00	Finalised	Shelim Miah	21/09/16

Authorisation:	
Name / Position	**Mark Duff/ Interim Director of IT Services**
Signature	**Mark Duff**
Date	**21/09/16**

CONTENTS

1 POLICY STATEMENT 4

DISCLAIMER 4

2 SCOPE 4

3 ACCOUNT CREATION 4

STUDENTS 5

STAFF 5

4 MANAGING ACCOUNTS 5

5 ACCESS PRIVILEGES 6

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

Disclaimer:

1.3 IT Services do not currently hold a single repository or database to maintain all the details of user accounts, their specific access privileges and their up-to-date status e.g. enabled/disabled.

1.4 IT Services do not currently have any process in place to review user access rights at appropriate/regular intervals or record any status change of a user e.g. promotion, demotion, termination, extension or change of role within QMUL.

1.5 IT Services understands that the above policy statements are highly recommended and are recognised as good practise by ISO standards, however IT Services is unable to comply due to technical or resourcing constraints. IT Services supports and advocates that departments where possible should make every effort to adhere to these policy statements.

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 information systems.

3 Account Creation

3.1 All new users must agree, to comply with QMUL's 'Conditions of Access to Computing Facilities. Agreement' policy can be by signature or electronically.

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 Polices, Regulations, Terms and Conditions.

Students

3.5 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.

3.6 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.

3.7 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

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

3.9 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.

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 reserves the right to 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 Where a student completes their study in June/July their account is disabled on 1st August, 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 or removed or extended, prior to termination depending on a risk assessment that 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 is accessible.

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 to ensure any personal data held in their IT account is transferred and/or deleted off the IT network before the account is disabled.

6.7 For any account to be extended a request must be made by the School Manager or equivalent detailing the reason for the account extension, the length of the extension is required for and before the account is disabled. The School Manager or equivalent will remain responsible and accountable for the account extension.

7 Guest Accounts

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

7.2 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).

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

7.4 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.

7.5 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.

7.6 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 may result in the IT Account and associated information system access being disabled.

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

12 Appendix A

12.1 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.
ITSB	IT Strategy Board – Team of Executive Managers consisting of Vice Principals and the IT Director, who oversee the delivery of the IT Strategy.
Account Sponsor	Can be a line manager or person of authority that is responsible and accountable for an IT Account that has been issued.