Standard Operating Procedures (SOP) for:			
Information Classification			
SOP Number:	**DG09**	Version Number:	**2.0**
Effective Date:	**07 Aug 2015**	Review Date:	**07/08/2018**

Author: Reviewer:	**Marion Rosenberg, Information Security Manager** **Paul Smallcombe, Records & Information Compliance Manager** **Information Governance Group**

Authorisation:	
Name / Position	**Chris Day, Director of IT Services**
Signature	**C Day**
Date	**14/02/2012**
Name / Position	**Wendy Appleby, Secretary to Council & Academic Secretary**
Signature	**Wendy Appleby**
Date	**15/07/2014**

Accountability:	
Position	Line Managers
Responsibility:	
Position	Owners of Information Assets

Revision History			
Version	Description	Author	Date
1	Initial version.	William Mordaunt	27/05/2010
1.1	Review	Marion Rosenberg	13/02/2012
1.2	Review and update of terminology	Paul Smallcombe	04/03/2014
2.0	Review and addition of Highly Confidential category	Paul Smallcombe	27/05/2015

Purpose and Objective:
To define standards for the classification of information assets for all data owned by QMUL. Information is one of the most valuable assets that QMUL has. QMUL also has a legal obligation to protect data against loss and unauthorised disclosure. In order to meet these obligations and protect this asset it is important that data is classified and managed accordingly.

SOP Text

	Responsibility	Activity
1.	Owners of Information Assets	Owners of information assets shall define the classification of their assets and periodically review them. The information classification is shown in Appendix A.
2.	Owners of Information Assets	Physical and electronic assets shall be labelled to show their classification where appropriate. Where labelling of electronic assets is not possible, other means of designating the classification shall be applied, e.g. via procedures or meta-data.

3.	Owners of Information Assets	The default control measures that shall be adopted for unmarked assets shall be as per those for the Protect information classification category.
4.	Owners of Information Assets	The classification of information assets may change after a period of time for example when superseded or when made public. Any change shall be approved by the owner.
5.	Owners of Information Assets / IT Services	The control measures used to protect information assets shall be appropriate to the information classification category. Example control measures are shown in Appendix A.
6.	Owners of Information systems	For Highly Confidential or Confidential systems or remote access to QMUL networks, two factor authentication should be used.
7.	Owners of Information Systems	Any system or application that is classified as Protect, Restricted, Confidential or Highly Confidential must have access control.

List of Appendices

Appendix	Appendix name	Location
Appendix A	Information Classification	On pages 3-4

Appendix A – Information Classification

Category	Description and Examples	Control Measures
Highly Confidential	Unauthorised disclosure (even within QMUL) or loss would cause extreme harm to the interests of QMUL or individuals, up to and including loss of life. • Information identifying individuals whose lives may be put at risk as a result	Contact IT Services for specialist advice; minimum should be as for Confidential. Physical assets labelled "Queen Mary University of London Highly Confidential"
Confidential	Unauthorised disclosure (even within QMUL) or loss would cause serious damage to the interests of QMUL or individuals. • Patient identifiable data or other sensitive personal data • Commercially exploitable research	Stored and transmitted in encrypted form and/or physically locked up Access restricted to staff requiring it for performance of their duties Physical assets labelled "Queen Mary University of London Confidential"
Restricted	Unauthorised disclosure (even within QMUL) or loss would cause significant harm to the interests of QMUL or individuals. • Employee and student records • Commercial contracts • Financial data • Student mark sheets	Stored in separate system folders or directories protected by passwords Usually transmitted in encrypted form Access restricted to staff requiring it for performance of their duties Physical assets labelled "Queen Mary University of London Restricted"
Protect	Unauthorised disclosure, particularly outside QMUL, would be inappropriate and inconvenient. • Information published on the QMUL intranet	Information restricted to QMUL staff/students
Open (Not protectively marked)	Information already in the public domain. • Information published on the QMUL public web site	No restrictions on access

	• Information that would be released in its entirety in response to a Freedom of Information request	

Integrity

Classification	Description
Guaranteed	Lack of integrity could cause QMUL Catastrophic financial, reputational or legal damage ➢ Student Marks ➢ Research Data
Assured	Lack of integrity could cause QMUL Major financial, reputational or legal damage
Standard	Lack of integrity could cause QMUL Moderate financial, reputational or legal damage
NA	There is no requirement for controls around the editing or updating of data

Availability

Classification	Description
Highly-Critical	If the information/ system was not available QMUL or business unit would be unable to continue with business until the system was recovered
Critical	If the information/system was not available QMUL or business unit could continue its business for a while but not indefinitely
Non-Critical	If the information/ system was not available QMUL or business unit could continue but at reduced efficiency
NA	Information/Service recovery timescale and impact is not defined or required