Queen Mary
University of London

Information/Data Governance Policy

DG09 - Information Classification

Prepared by: < >
Version: 2.0

Effective Date:	**28/05/2018**	Review Date:	**28/05/2021**

Reviewers:	**Ian Douglas, Information Security Manager** **Paul Smallcombe, Records & Information Compliance Manager** **Information Governance Group**
Policy Owner:	
Name/Position	Rhys Davies, Chief Information Officer

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
1.3	Review and addition of Highly Confidential category	Paul Smallcombe	27/05/2015
1.4	Updated Template	Shelim Miah	15/05/2017
1.5	Updates	Paul Smallcombe	17/05/2017
2.0	Final Version	Shelim Miah	28/05/2018

Authorisation:	
Name / Position	Rhys Davies, Chief Information Officer
Signature	**R. Davies**
Date	**28.05.2018**

Contents

1. Policy Statement

1.1. This policy ensures all information held by QMUL is assessed and classified to determine its sensitivity, so that it is appropriately protected and can only be accessed by those who are authorised to do so.

1.2. The Policy aims to:

- Outline the expectations of those creating and handling information.
- Ensure the security and protection of QMUL data.
- The Appropriate level of sensitivity of information is recognised
- Outline roles & responsibilities
- Enhance Communications

2. Scope

2.1. This policy applies to all staff, students, third party suppliers, contractors and visitors who have access to or create data/information that is owned or held by QMUL. This includes both physical media and electronic data/information stored on any devices that may or may not be owned by QMUL for example information in the cloud. This also includes documents that have been printed, written notes on paper and webpages.

3. Policy Detail

3.1. Information assets need to be identified and assigned an owner who will be accountable for ensuring the adequate classification and labelling of the Information asset.

3.2. The owners of information assets must define the classification of their assets and periodically review them.

3.3. Only the author or the designated information owner can apply the protective marking to their information asset. If the author is not known or not contactable or it is uncertain what classification is to be used, the matter is to be referred to the Information Governance Group (IGG) and or the Information and Records Compliance Manager to help track down a suitable owner.

3.4. Physical and electronic assets must be labelled to show their classification where appropriate e.g. footer of a document. Where labelling of electronic assets is not possible, other means of designating the classification shall be applied, e.g. via procedures or meta-data, verbally informing of the classification.

3.5. Information Classification is to be used to:

- Determine the level of protection needed for the information/data
- Indicate that level of protection to other people
- Establish a consistent approach to ensuring that data is appropriately protected.

3.6. QMUL uses four protective marking which are;

- **Highly Confidential** – Information that an 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.
- **Confidential** - Information that an unauthorised disclosure (even within QMUL) or loss would cause serious damage to the interests of QMUL or individuals
- **Restricted** – Information that an unauthorised disclosure (even within QMUL) or loss would cause significant harm to the interests of QMUL or individuals.
- **Protect** – Information that an unauthorised disclosure, particularly outside QMUL, would be inappropriate and inconvenient to QMUL and its staff/students.
- **Open** - any document not containing sensitive information shall be marked with Open, this is usually information that is already out in the public domain

3.7. Where the integrity and availability of the information must be maintained, additional classifications are available in the appendix for determining the level of Integrity and availability classification of the information.

3.8. The default control measures that shall be adopted for unmarked assets will be as per the 'Protect' information classification category.

3.9. The classification of information assets may change over a period of time, Information assets need to be reviewed to ensure the information asset maintains the appropriate marking, for example when superseded or when made public.

3.10. The information owner must approve any changes in classification.

3.11. Control measures must be in place as defined in appendix that is appropriate to protect the information asset.

3.12. For Highly Confidential or Confidential systems or remote access to QMUL networks, two-factor authentication must be used.

3.13. Any system or application that is classified as Protect, Restricted, Confidential or Highly Confidential must have access control.

3.14. Any system or application that is classified as Protect, Restricted, Confidential or Highly Confidential must be recorded in the Information Asset register and registered with the Information & records Compliance manager

3.15. Where Information is required to be transferred or moved, this must be done in accordance to the DG015 Handling of information policy.

3.16. In the event information asset is compromised or suspected of being compromised, this shall be reported to the information owner to take the appropriate action as defined in DG05 – IS Incident reporting.

4. Roles & Responsibilities

4.1. The Risk and Governance Manager will be the custodian of the document and manage its review and update. All approved documentation are to be stored in a central repository and uploaded to the web where applicable.

4.2. The Information Governance Group (IGG) will own and authorise the change and release of this document.

4.3. All information (document) owners are responsible for classifying and labelling their document.

4.4. All staff/students and individuals who have access to QMUL information assets have a responsibility to abide by the classification of the asset.

5. Process and Procedures

5.1 The associated processes and guidance documents can be found by visiting the **ITS webpage** and the **Information Governance Webpage**

6. Monitoring

6.1. It is mandatory for all information asset owned or held by QMUL to comply with this Policy and any associated procedure. Where non-compliance is identified, appropriate action will be taken, which may result in escalation to senior management.

6.2. Checks may be made by the Risk and Governance Manager or the Head of Information Security and the findings may be reported to the IT Lead Team (ITLT) and or IGG for corrective actions to be issued.

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 IGG for a decision via the Records & Information Compliance Manager.

7.2. The IGG will then make a decision or refer this to Queen Mary Senior Executive team (QMSE) for guidance.

8. References

SOP DG25 – Configuration Management & Change Control
SOP DG09 – Information Classification

9. 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. Access restricted to staff requiring it for performance of their duties. The integrity of the data needs to be Guaranteed 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. The integrity of the data needs to be Guaranteed 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. The integrity of the data needs to be Assured. 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 • Internal correspondence • Committee papers and minutes	Information restricted to QMUL staff/students Formatting information to provide basic security, such as converting Word doc into pdf to avoid tampering. The integrity of the data needs to be at Standard.
Open (Not protectively marked)	Information already in the public domain. • Information published on the QMUL public web site • Information that would be released in its entirety in response to a Freedom of Information request	No restrictions on access Formatting information to provide basic security, such as converting Word doc into pdf to avoid tampering.

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

10. Definitions

Term	Meaning
Information Asset	Where valuable information or data that can be sensitive is captured and stored, this can be systems, physical paper, CD and mobile devices such as SD cards, pen drives etc.
Data Sets	A collection of data or information that could be contents of a database or a project file
Risk	An uncertain event or circumstance that, if it occurs, will affect the outcome of an objective
Process	A series of actions or steps taken in order to achieve a particular outcome
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.
IGG	Information Governance Group – provide assurance and guidance on information governance across QMUL.
QMSE	Queen Mary Senior Executive (QMSE) is Queen Mary's senior management team who advise the Principal on the management of day-to-day business as well as its long-term future. The group comprises the Principal, Vice-Principals and the Senior Officers in Professional Services
User	A member of staff, enrolled student, contractor, visitor, or another (any other) person authorised to access and use QMUL's systems.