Queen Mary
University of London

Information/Data Governance Policy

DG16 – Disposal of Information - Policy

Prepared by: < Shelim Miah>

Version: 2.0

Description & Target Audience:			
Effective Date:	**Feb 2018**	Status:	**Active**

Reviewers:	David Boakes, Assistant Director IT Operations Paul Smallcombe, Records & Information Compliance Manager Ian Douglas, Chief Information Security Officer
Policy Owner:	
Name/Position	Paul Smallcombe

Revision History

Version	Description	Author	Date
1	Initial version.	Benjamin Roberts	22/04/2010
1.1	Annual Review – Small changes	Paul Smallcombe	15/05/2014
1.1	Annual Review – No Change	Paul Smallcombe	29/05/2015
1.2	Updates	Shelim Miah	11/05/2017
1.3	Updates	Paul Smallcombe	19/05/2017
1.4	Draft Finalised	Shelim Miah	12/06/2017
2.0	Finalised	Shelim Miah	15/01/2018

Authorisation:	
Name / Position	Information Governance Group
Signature	
Date	

Contents

1. Policy Statement

1.1. One of the most valuable assets that QMUL has is its information. It is important to capture and store this information in line with QMUL information governance and retention Policies. QMUL has a legal obligation to protect this information against loss and unauthorised disclosure. In order to meet these obligations and protect this asset, it is important that information be managed so that it is classified, stored, handled and disposed of according to its classification.

1.2. This policy ensures that all information held by QMUL in all formats and media must be disposed of appropriately according to its classification, business requirements and retention period, such that this information is protected from unauthorised access or misuse.

1.3. The Policy aims to:

- Outline the expectations of those who store and handle information.
- Ensure the security and protection of QMUL information.
- Ensure sufficient controls are in place to minimise the risk of information being compromised.
- Outline roles & responsibilities.
- Enhance communications.

2. Scope

2.1 This policy applies to all QMUL staff who have access to data/information that may or may not be of a sensitive nature, including any third party who stores, holds and has access to data for QMUL.

3. Policy Detail

3.1. All devices and media (electronic & physical) are checked prior to disposal for any Highly Confidential, Confidential or Restricted information, as defined in DG09 – Information Classification and the disposal process will ensure that this information cannot be recovered.

3.2. All damaged devices containing information shall be subject to a risk assessment prior to being removed off site for repair.

3.3. A record is to be kept of all information and media that has been disposed of, this would normally be the information holder.

Disposal of physical Highly Confidential, Confidential or Restricted information

3.4. Paper records or other physical records, such as film, microfilm are to be destroyed by shredding (via use of confidential waste bins where available) or otherwise physically destroyed such that the information cannot be recovered.

3.5. Where the Highly Confidential, Confidential or Restricted information consists of personal information, any third party performing disposal on behalf of QMUL must be contracted under the terms of a data processor agreement.

Disposal of electronic Highly Confidential, Confidential or Restricted information

3.6. When electronic data is to be destroyed simply formatting a disk drive is not adequate. To ensure secure deletion, a product that overwrites data many times must be used, such that the information cannot be recovered. The QM IT Security Team will provide guidance and advice about the use of these products.

3.7. Media and devices holding electronic data including, but not limited to CDs, DVDs, tapes, diskettes, flash memory devices, and PDAs, are to be either physically destroyed or disposed of via a company that specialises in secure data destruction, that will collect the hardware and ensure all data thereon is destroyed. See DG10 – IT Equipment Disposal. IT Services shall provide departments with details of suitable disposal companies on request.

3.8. Where a third party performs any destruction on behalf of QMUL, they must provide a certificate confirming destruction.

3.9. Where the Highly Confidential, Confidential or Restricted information consists of personal information, the third party must be contracted under the terms of a data processor agreement.

4. Roles & Responsibilities

4.1. The Risk and Governance Manager will be the custodian of this policy and manage its review and update. All approved documentation is 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 policy.

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

4.4. Information owners are responsible for the handling, storage, disposal and management of information assets in their care. For electronic ITS maybe involved in the disposal.

5. Process and Procedures

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

6. Monitoring

6.1. It is mandatory for all information assets 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 for action to be taken.

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 DG09 – Information Classification
SOP DG10 – IT Equipment Disposal

9. Definitions

Term	Meaning
Information Asset	A piece of information such as a document, record or report that holds data that is valuable and can be sensitive.
Physical Data	These include but not limited to items like Micro fiche/film and paper
Electronic Data	These include but not limited to CD, DVDs, USB and Disk drives
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