Information/Data Governance Policy

DG15 – Handling Information - Policy

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.	Benjamin Roberts	28/05/2010
1	Annual Review – No change	Paul Smallcombe	09/05/2014
1.1	Annual Review – minor changes	Paul Smallcombe	29/05/2015
1.2	Minor Changes based on feedback from Paul	Ian Douglas	21/07/2015
1.3	Update	Shelim Miah	11/05/2017
1.4	Updates	Paul Smallcombe	09/06/2017
1.5	Draft Finalised	Shelim Miah	12/09/2017
2.0	Reviewed	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 in all formats and media must be handled appropriately according to its classification DG09 – Information Classification, such that this information is protected from unauthorised disclosure or misuse.

1.2. The Policy aims to:

- Outline the expectations of those who store and handle information.
- Ensure the security and protection of QMUL information.
- Sufficient controls are in place to minimise the risk of compromising information
- Outline roles & responsibilities
- Enhance Communications

2. Scope

2.1. This policy applies to all staff who have access to or wish to have access to data/information that is of a sensitive nature, including any third party who store or hold data for QMUL.

3. Policy Detail

3.1. All Information must be stored in suitable storage as per DG14 – Storage of Information and protected accordingly to prevent unauthorised access.

3.2. All forms of media and documentation that hold Data or Information must be labelled to indicate the classification of Open, Protect, Restricted, Confidential and Highly Confidential as defined in DG09 – Information Classification.

3.3. The distribution of Highly Confidential, Confidential or Restricted information must be kept to a minimum and distributed only where necessary.

3.4. A record of those authorised to access or receive Highly Confidential, Confidential or Restricted information must be maintained and reviewed on an annual basis.

3.5. The information owner must authorise the dispatch or removal of information under their responsibility.

3.6. Intended recipients of information must be authorised to receive the information, especially if it is sensitive information.

3.7. Before sending information, the sender must ensure that third party recipients of the information have suitable policies and procedures in place to ensure the confidentiality and integrity of the information.

3.8. Third parties in receipt of information must maintain the required confidentiality and integrity of that information asset in accordance to QMUL's information governance policies or higher.

Transmitting information

3.9. Information must only be transmitted across networks when the required confidentiality and integrity of the information can be assured throughout the transfer.

3.10. Highly Confidential, Confidential or Restricted information transmitted electronically by computer across networks must be encrypted and password protected.

3.11. To gain access to Highly Confidential, Confidential and Restricted information across the general internet enhanced authentication is to be used as per DG19 Remote Access Policy.

3.12. Advance warning of Highly Confidential, Confidential and Restricted information must be sent to all recipients to allow them to prepare suitable storage to receive the information being sent.

3.13. All recipient details including third parties are to be checked prior to sending any type of data to ensure information does not fall into the wrong hands.

Transporting Information

3.14. Highly Confidential, Confidential or Restricted information transported physically in the form of removable media or a mobile computing device, must be encrypted.

3.15. Hard copies of Highly Confidential, Confidential or Restricted information shall be handled appropriately. Removal off site must be authorised by an appropriate manager and a record kept of this authorisation.

3.16. Prior to authorisation, a risk assessment based on the criticality of the information asset shall be carried out.

3.17. Physical media containing Highly Confidential, Confidential or Restricted information in transit must be protected as follows:

a) reliable transport or couriers should be used;
b) a list of authorised couriers must be agreed with management;
c) couriers must be identified;
d) packaging must protect the contents from any physical damage;
e) controls to protect information using the following methods
   - use of locked containers
   - delivery by hand
   - tamper-evident-packing
   - double-layered packing
   - in exceptional cases, the consignment shall be split into more than one delivery and dispatched by different routes.

Loss of Information

3.18. Information owners must ensure that appropriate backup, recovery and archival procedures are in place.

3.19. Where an information security incident occurs or is suspected of occurring such as where handling leads to leak or loss of information, the incident must be managed and reported as per DG05 – Information Security Incident Reporting.

3.20. The Information Security Manager, Information owner and the Records & Information Compliance Manager must be informed of the incident or potential incident.

Access to Personal Information

3.21. Due care must be taken when it is necessary for any person who is not the normal user to access a user's email account, home drive or any such personal data.

3.22. The QM IT Security Team shall provide advice as necessary to any person engaged or considering such an intrusion.

3.23. The QM IT Security Team must be prepared to act as a disinterested third party in any such cases to reduce the degree of intrusion and ensure that proper logging of the intrusion takes place.

3.24. Any form of interception or monitoring of communications on the QMUL network or systems is strictly prohibited unless explicitly authorised by an appropriate person and may result in disciplinary proceedings and/or constitute a criminal offence under the Regulation of Investigatory Powers Act 2000

3.25. NB: The RIPA and Lawful Business Practice Regulations 2016 do allow for legitimate interceptions of communications by organisations on their private computer and telecommunications networks - in other words, they provide 'lawful authority'.

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 information.

4.4. Information owners are accountable for their information but responsibility may be delegated to the Data Custodian. i.e. the HR director owns HR data and is accountable for it but the AD Applications is the Data Custodian and is responsible for the data protection in the HR system.

5. Process and Procedures

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

5.2. The following documentation should be consulted in the event of a loss or compromise of information:

a) DG05-Information Security incident reporting

b) DG27 IT Security Incident Reporting

5.3. For further guidance the Chief Information Security Officer or the Records & Information Compliance Manager should be consulted.

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 DG05 – IS Incident Reporting
SOP DG09 – Information Classification
SOP DG12 – Cryptographic Controls
SOP DG14 – Storage of Information
SOP DG26 – System Backup and Recovery

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.
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