Information/Data Governance Policy

DG14 – Storage of Information

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	Updates	Shelim Miah	11/05/2017
1.4	Updates	Paul Smallcombe	05/06/2017
1.5	Draft Finalised for approval	Shelim Miah	12/06/2017
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 are stored securely according to the classification set out in DG09 – Information Classification. Storage Measures must be in place so that this information is protected from unauthorised access, 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 users who have access to or wish to have access to data/information that may or may not be of a sensitive nature, including any third party who store or hold data for QMUL.

3. Policy Detail

3.1. Information that is held must be secured against loss, damage and unauthorised access or modification.

3.2. Information shall be accessible to authorised users when they require it.

3.3. All Highly Confidential, Confidential and Restricted information shall be access-controlled in accordance with DG11 – System Access Controls. This applies to information in all forms.

Storage of Electronic Information

3.4. Highly Confidential, Confidential and Restricted information must not be stored on mobile devices or removable media (e.g. USB sticks, laptop computers, mobile phones etc.) and non-mobile storage not in a physical secure area (i.e. NAS Device, Server attached storage etc.) unless it is encrypted.

3.5. Where information is stored on mobile devices (USB, laptops, tablets etc.), special care must be taken to ensure that the device is protected from theft, loss or damage.

3.6. Information must be regularly backed up, all back-ups must be stored under the same secure conditions as the live information.

3.7. Information must be stored on or in equipment and/or in locations that are sited or protected to reduce the risks from environmental threats and hazards and opportunities for unauthorised access or other damage.

3.8. Information must be stored on or in equipment protected from power failures and other disruptions caused by failures of supporting utilities.

3.9. Electronic information must be checked every five years or when there is a system upgrade, whichever is soonest, to ensure that it can still be accessed.

3.10. Information storage capacity should be reviewed frequently at least annually and where necessary increased to meet demands.

3.11. Information must be stored in accordance to the retention policy and retention schedule.

3.12. Sensitive information is not to be stored on cloud services, using third party cloud services to store information may not be secure and carries risks, the Cloud Guidance document provides further detail on the use of cloud storage.

3.13. Information is not to be stored on personal email accounts.

3.14. Research and clinical data must be stored and handled in accordance with the General data Protection Regulation (GDPR) and the Medicines and Healthcare products Regulatory Agency (MHRA).

Storage of Physical Information

3.15. Paper based information storage should be adequately protected against unauthorised access as well as from damage that can be caused by vermin, fire, water and other natural disasters.

3.16. Paper based information should be locked in cabinets and key held with nominated individuals. Where the information is Highly Confidential, Confidential and Restricted the keys must be signed in and out and all key holders must be documented.

3.17. Copies of Highly Confidential, Confidential and restricted must not be made without the information owner's permission. Where permission is granted, the number copies made; by whom and where held must be documented and registered with the Records and Compliance Manager.

Information Access

3.18. Access to the sensitive information must be controlled and only made available to those who are authorised to do so as part of their role within QMUL.

3.19. Users accessing sensitive information must be identifiable and where possible logged so that it is clear who accessed the information and for how long and for what purpose.

3.20. Users who have been authorised access must not pass on or relay information to others who have not been authorised to receive or view that information.

3.21. Where the authorised user no longer requires access to the information or has changed roles, their access is to be revoked and passwords changed where necessary.

3.22. All appropriate steps including assessments on the suitability of access to information must be carried out before allowing access

3.23. Where information is to be disclosed or published, ensure the anonymity of individuals is maintained in accordance to the data protection legislation. This can be done where necessary by redacting information or De-identification.

3.24. Sensitive information must not be accessed using personal devices or over public internet services.

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. Information owners are responsible for the handling, storage and management of information assets in their care.

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.

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 DG09 – Information Classification
SOP DG11 – System Access Controls
SOP DG12 – Cryptographic Controls
SOP DG13 – Records Management

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
Radacting	Removing or blocking personal or sensitive information in a document.
De-identification	The separation or replacement of information in a data set which prevents the ability to link a data set to the identity of a person