Queen Mary
University of London

Information/Data Governance Policy

DG09 - Information Classification

Prepared by: < >
Version: 3.5

Effective Date:	**23/02/2022**	Review Date:	**23/02/2024**

Reviewers:	**Paul Smallcombe, Records & Information Compliance Manager** **Information Governance Group**
Policy Owner:	
Name/Position	Information Governance Group

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 classification 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
2.1	Updates from reviews by P. Smallcombe	Shelim Miah	06/07/2020
2.2	Updated Appendix A	Paul Smallcombe	17/02/2021
2.3	Moved PII to Highly Confidential classification category	Paul Smallcombe	26/04/2021
3.0	Merger of associated policies and revision of Appendix A	Paul Smallcombe	12/12/2021
3.1	Addition of Information Storage Matrix at Appendix B	Paul Smallcombe	24/06/2022
3.3/3.4	Minor revisions to Appendix B	Paul Smallcombe	19/12/2023
3.5	Addition of Enterprise Dropbox	Paul Smallcombe	29/02/2024

Authorisation:	
Name / Position	**Information Governance Group**
Signature	***Information Governance Group***
Date	**19/04/2022**

Contents

1. Policy Statement

1.1. This policy aims to ensure that all information held by QMUL is assessed and classified to determine its sensitivity, so that it is protected, handled and disposed of appropriately and can only be accessed by those who are authorised to do so and in line with legislation.

1.2. The Policy aims to:

- Outline the expectations of those creating, handling, storing and disposing of information
- Ensure the security and protection of QMUL data
- Ensure that the appropriate level of sensitivity of information is recognised
- Ensure controls are in place to minimise the risk of information security incidents
- Outline roles and 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. Information Classification

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 Records & Information Compliance Manager to help identify 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 metadata, 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 five classifications for protective marking, which are:

- **Highly Confidential** – Information where an unauthorised disclosure (even within QMUL) or loss of which would cause extreme harm to the interests of QMUL or individuals, up to and including loss of life.
- **Confidential** – Information where an unauthorised disclosure (even within QMUL) or loss of which would cause serious harm to the interests of QMUL or individuals.

- **Restricted** – Information where an unauthorised disclosure (even within QMUL) or loss of which would cause harm to the interests of QMUL or individuals.
- **Protect** – Information where an unauthorised disclosure, particularly outside QMUL, or loss of which would be inappropriate and/or inconvenient to QMUL and its staff/students.
- **Open** – Any other information, the disclosure or loss of which would not cause any of the harms described above, shall be marked with Open. This is usually information that is suitable to be or is already in the public domain.

3.7. Where the integrity and availability of the information must be maintained, additional classifications are available in Appendix A 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 A that are appropriate to protect the information asset.

3.12. For systems processing information classified as Highly Confidential or Confidential, or remote access to QMUL networks, multi-factor authentication (MFA) 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 an Information Asset Register and notified to the Records & Information Compliance Manager.

3.15. In the event an 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 – Information Security Incident Reporting.

4. Information Storage

4.1. Information that is held must be secured against loss, damage and unauthorised access or modification. Information must be stored in suitable means that is appropriate to its classification.

Storage of Electronic Information

4.2. Highly Confidential, Confidential and Restricted information must not be stored on mobile devices or removable media (e.g. USB sticks, laptop computers, mobile phones, tablets etc.) and non-

mobile storage that is not in a physically secure area (i.e. NAS device, server attached storage, etc.) unless it is encrypted.

4.3. Where information is stored on mobile devices or removable media, special care must be taken to ensure that the device is protected from theft, loss, or damage.

4.4. Information must be regularly backed up; all back-ups must be stored under the same secure conditions as the current/live information.

4.5. 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, loss, or other damage.

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

4.7. 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.

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

4.9. Information must be stored in accordance with the Records Retention Policy and Retention Schedule.

4.10. Information must not be accessed or stored on personal (non-QMUL) accounts with third parties (e.g. GMail, Dropbox, iCloud).

4.11. Users should refer to Appendix B for further guidance.

Storage of Physical Information

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

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

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

Information Access

4.15. Access to information classified as Protect and above must be controlled and only made available to those who are authorised to do so as part of their role within Queen Mary.

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

4.17. 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.

4.18. 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.

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

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

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

5. Information Handling

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

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

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

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

5.5. 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.

5.6. Third parties in receipt of information must maintain the required confidentiality and integrity of that information asset in accordance with Queen Mary's information governance policies or higher.

Transmitting information

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

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

5.9. 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.

5.10. 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.

5.11. 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

5.12. Highly Confidential, Confidential or Restricted information transported physically in the form of removable media or a mobile device, must be encrypted and password protected where possible.

5.13. 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.

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

5.15. 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 when taking custody;
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

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

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

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

6. Information Disposal

6.1. All devices and media (electronic & physical) are to be checked prior to disposal for any Highly Confidential, Confidential or Restricted information and the disposal process must ensure that this information cannot be recovered.

6.2. The disposal of information shall only be carried out after due consideration of relevant retention policies.

6.3. All damaged devices containing information shall be subject to a risk assessment prior to being removed off site for repair, to ensure that the information is not subject to misuse and/or able to cause potential harm to an individual or an organisation including Queen Mary.

6.4. A record shall be kept of all information and media that has been disposed of, ordinarily by the information holder.

Disposal of electronic Highly Confidential, Confidential or Restricted information

6.5. When electronic data is to be destroyed, simply formatting a 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. IT Services can provide guidance and advice about the use of these products.

6.6. Media and devices holding electronic data including, but not limited to CDs, DVDs, tapes, diskettes, flash memory devices, hard drives and tablets, 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.

6.7. Where a third party performs any destruction on behalf of Queen Mary, they must provide a certificate confirming destruction.

6.8. 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.

6.9. Where a damaged device is sent for repair that contains Highly Confidential, Confidential or Restricted information, this should be first removed where possible, however if removal is not possible, the company carrying out the repair should be contracted under the terms of a data processor agreement if the device may hold personal information.

Disposal of physical Highly Confidential, Confidential or Restricted information

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

6.11. Where a third party performs any destruction on behalf of Queen Mary, they must provide a certificate confirming destruction.

6.12. 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.

6.13. Confidential waste must be kept separate from other waste material and must be clearly labelled or bagged as confidential waste.

6.14. Bagged confidential waste must be kept secure until collection.

7. Roles & Responsibilities

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

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

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

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

8. Process and Procedures

8.1 The associated processes and guidance documents can be found by visiting the ITS Webpage and the Information Governance Webpage.

9. Monitoring

9.1. It is mandatory for all information assets owned or held by Queen Mary to be done so in compliance 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.

9.2. IT Services may request checks to be carried out as part of internal audits and any findings may be reported to the IT Lead Team (ITLT) and or IGG for corrective actions to be issued.

10. Exceptions

10.1. 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.

10.2. The IGG will then make a decision or refer this to Queen Mary Senior Executive Team (SET) for guidance.

11. References

11.1. SOP DG05 – Information Security Incident Reporting
SOP DG25 – Configuration Management & Change Control
SOP DG14 – Storage of Information (now retired & superseded by this document)
SOP DG15 – Handling of Information (now retired & superseded by this document)
SOP DG16 – Disposal of Information (now retired & superseded by this document)

12. Appendix A - Information Classifications

Classification Category	**Open**	**Protect**	**Restricted**	**Confidential**	**Highly Confidential**
Risk Level	None	Low	Medium	High	Critical
Description	Suitable to be or already in the public domain	Unauthorised disclosure or loss, particularly outside Queen Mary, would be inappropriate and/or inconvenient	Unauthorised disclosure (potentially even within Queen Mary) or loss would cause harm to the interests of Queen Mary or individuals	Unauthorised disclosure (even within Queen Mary) or loss would cause serious harm to the interests of Queen Mary or individuals	Unauthorised disclosure (even within Queen Mary) or loss would cause extreme harm to the interests of Queen Mary or individuals, up to and including loss of life
Control Measures†	No restrictions on access. Available to anyone, anywhere in the world. Formatting information to provide basic security, such as converting Word doc into PDF to avoid tampering, as necessary.	Information restricted to Queen Mary 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. Assets marked "Queen Mary University of London Protect".	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. Assets labelled "Queen Mary University of London Restricted": physical by labelling; electronic marked in a file name (and/or other metadata field in the Properties) and/or in the header or	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. Assets labelled "Queen Mary University of London Confidential": physical by labelling; electronic marked in a file name (and/or other metadata field in the Properties) and/or in the header or footer of a	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. Assets labelled "Queen Mary University of London Highly Confidential": physical by labelling; electronic marked in a file name (and/or other metadata field in the Properties) and/or in the header or footer of a

			footer of a document, emails marked in the subject line. Disposed of in a secure manner, such as via confidential waste facility.	document, emails marked in the subject line. Disposed of in a secure manner, such as via confidential waste facility.	document, emails marked in the subject line. Disposed of in a secure manner, such as via confidential waste facility.
Examples* (not exhaustive)	• Information published on the Queen Mary public web site • Information that would be released in its entirety in response to a Freedom of Information request • Published research • Course catalogues • Published faculty and staff information • Policies • Marketing information	• Information published on the Queen Mary intranet • Internal correspondence • Departmental procedures • Employee web/intranet portals • Training materials • Drafts of research papers • Committee papers, agendas and minutes • Project information	• Employee and student records • Commercial contracts • Financial data • Student mark sheets	• Other special category personal data • Personal data relating to criminal convictions and offences • Commercially exploitable research • Passwords and PINs • System credentials • Private encryption keys • Government issued identifiers (e.g. National Insurance Number, Passport number, driver's license copy) • Individually identifiable financial account information (e.g. bank account, credit or debit card numbers)	• Information identifying individuals whose lives may be put at risk as a result • Patient Identifiable Information • Details of significant security exposures (e.g. vulnerability assessment and penetration test results) • Security system procedures and architectures • Systems managing critical Operational Technology

				• A list of personal characteristics or other information that would make an individual student's identity easily traceable • Individually identifiable research data • Patent applications • Grant applications	

†More specific guidance can be found by consulting Appendix B.
*More specific examples can be found in column E of the QMUL Records Retention Schedule.

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

13. Appendix B - Information Storage Matrix

This Matrix is best viewed as an Excel spreadsheet available from https://www.qmul.ac.uk/governance-and-legal-services/media/arcs/governance/information-governance/Information-Storage-Matrix-v.01.3.xlsx

	Storage Description	Storage on a fixed self-managed desktop PC i.e. hard drive and or Network Attached Storage (NAS), kept inside QMUL with locally held data intended for permanent storage	Hard Drive in a fixed managed desktop PC with locally held data intended for permanent storage. This includes ITS and School Managed Devices	Encrypted Hard Drive on an ITS managed device (if intended for permanent storage)	Authorised Data Safe Haven environ-ments (BCC, UKSeRP)	Self-managed portable device (and Research Managed Laptop virtual machines)	SharePoint MS Office 365 cloud	OneDrive MS Office 365 cloud	Dropbox for Business	Other cloud storage / SaaS provider	ITS authorised managed applications	NetApp (J/G drive) QM legacy end-user and departmental storage in QM's ME data centre	ITS Research High Performance Computing Research Storage	Encrypted portable media such as external hard drives and USB sticks (as approved by QM)
Type of Information and Classification	**Additional Information**	Also includes BYOD (personally owned laptop and/or PC). Note lack of backup	e.g. SEF devices with access to ONS data	Accessible on & off campus via VPN, uses QM credentials	Accessible on & off campus via VPN, uses independent credentials	Owned by QMUL but managed by keeper, used anywhere	This is the default storage location to share data between staff /Depts /students. It is available from any location and protected by MFA	This is the default storage location for almost all staff and students. It is available from any location and protected by MFA	Managed solution, available by exception on application. Protected by MFA	Where QMUL does not have a formal contract e.g. Google, free of charge/personal Dropbox, iCloud, box.com, etc.	Web-based application sanctioned by QMUL, e.g. SITS, Worktribe, QMPlus, echo360, LabArchives, Resourcelink, Wiseflow, Oleeo, Agresso, Online Surveys, Qualtrics, E-appraisal, Labnotes, OverLeaf	QM internal networks only and Managed devices including VDI	Available anywhere using SFTP, SCP and RSync	

Highly Confidential Patient identifiable information including research data from any research involving human participants (including data or human tissue) held under a current ethical approval	Forbidden	Forbidden	Forbidden	Permitted	Forbidden	Permitted with auditable additional measures	Forbidden	Forbidden	Forbidden	Forbidden	Forbidden	Forbidden	Forbidden
Highly Confidential Research data from any research involving human participants (including data or human tissue) held under a current ethical approval that contains pseudonymised special category personal data	Forbidden	Forbidden	Forbidden	Permitted	Forbidden	Permitted with auditable additional measures	Forbidden	Forbidden	Forbidden	Forbidden	Forbidden	Permitted with auditable additional measures	Forbidden
Highly Confidential Any other information the loss or public disclosure of which would cause harm to life	Forbidden	Permitted with auditable additional measures	Permitted with auditable additional measures	Permitted	Forbidden	Permitted with auditable additional measures	Forbidden	Forbidden	Forbidden	Forbidden	Forbidden	Forbidden	Permitted with auditable additional measures
Highly Confidential Information relating to significant security exposures, security system procedures and architectures and about systems managing critical Operational Technology (e.g. Estates and IT Services)	Forbidden	Forbidden	Forbidden	Permitted	Forbidden	Permitted with auditable additional measures	Permitted with auditable additional measures	Forbidden	Forbidden	Forbidden	Permitted with auditable additional measures	Forbidden	Forbidden
Confidential Research data from any research involving human participants held under a current ethical approval that contains personal data, including pseudonymised data but not including any special category personal data	Forbidden	Permitted with auditable additional measures	Forbidden	Permitted	Forbidden	Permitted	Permitted	Permitted	Forbidden	Permitted	Permitted	Permitted	Forbidden

Confidential Research grant applications	**Forbidden**	**Forbidden**	**Forbidden**	**Permitted**	**Forbidden**	**Permitted**	**Permitted**	**Permitted**	**Forbidden**	**Permitted**	**Permitted**	**Forbidden**	**Forbidden**
Confidential Sensitive research (e.g. BSU, defence, terrorism, etc.)	**Forbidden**	**Permitted with auditable additional measures**	**Permitted with auditable additional measures**	**Permitted**	**Forbidden**	**Forbidden**	**Forbidden**	**Forbidden**	**Forbidden**	**Permitted**	**Permitted with auditable additional measures**	**Forbidden**	**Permitted with auditable additional measures**
Confidential Non-research information which includes government identifiers (e.g. NHS Number, passport ID, etc.) or special category personal data (e.g. ethnicity, disability)	**Forbidden**	**Forbidden**	**Forbidden**	**Permitted**	**Forbidden**	**Permitted**	**Permitted**	**Permitted**	**Forbidden**	**Permitted**	**Permitted**	**Forbidden**	**Forbidden**
Confidential Credentials (e.g. passwords and PINs) for services hosting lower classifications NOT higher	**Forbidden**	**Forbidden**	**Forbidden**	**Permitted**	**Forbidden**	**Permitted with auditable additional measures**	**Permitted with auditable additional measures**	**Forbidden**	**Forbidden**	**Permitted**	**Permitted with auditable additional measures**	**Forbidden**	**Forbidden**

Confidential Financial information relating to the university (e.g. accounts, permissions to raise POs etc, banking details)	Forbidden	Forbidden	Forbidden	Permitted	Forbidden	Permitted	Permitted	Permitted	Forbidden	Permitted	Permitted	Forbidden	Forbidden
Confidential Examinable material prior to assessment	Forbidden	Permitted	Permitted	Permitted	Forbidden	Permitted	Permitted	Permitted	Forbidden	Permitted	Permitted	Forbidden	Permitted
Restricted Research data from any research involving human participants (including data or human tissue) held under a current ethical approval that contains no personal data (including truly anonymised data)	Forbidden	Forbidden	Forbidden	Permitted	Permitted	Permitted	Permitted	Permitted	Forbidden	Permitted	Permitted	Permitted	Forbidden
Restricted Research data not generated from research involving human participants (including data or human tissue)	Forbidden	Forbidden	Forbidden	Permitted	Permitted	Permitted	Permitted	Permitted	Forbidden	Permitted	Permitted	Permitted	Forbidden

Restricted Student and employee data (e.g. records of attendance and marks, appraisals, but not including any special category personal data)	Forbidden	Forbidden	Forbidden	Permitted	Forbidden	Permitted	Permitted	Permitted	Forbidden	Permitted	Permitted	Permitted	Forbidden
Restricted Day to day financial records (e.g. reports exported from Agresso)	Forbidden	Permitted	Permitted	Permitted	Forbidden	Permitted	Permitted	Permitted	Forbidden	Permitted	Permitted	Forbidden	Permitted
Restricted Contracts with external parties	Forbidden	Permitted	Permitted	Permitted	Forbidden	Permitted	Permitted	Permitted	Forbidden	Permitted	Permitted	Forbidden	Permitted
Protect Course lecture notes	Forbidden	Permitted	Permitted	Permitted	Permitted	Permitted	Permitted	Permitted	Forbidden	Permitted	Permitted	Forbidden	Permitted

Protect Recorded videos of lectures not containing commercially sensitive nor personal data	Forbidden	Permitted	Permitted	Permitted	Permitted	Permitted	Permitted	Permitted	Forbidden	Permitted	Permitted	Forbidden	Permitted
Protect Research data not containing sensitive nor personal data	Forbidden	Forbidden	Forbidden	Permitted	Permitted	Permitted	Permitted	Permitted	Forbidden	Permitted	Permitted	Permitted	Forbidden
Protect Research outputs in production or under review	Forbidden	Forbidden	Forbidden	Permitted	Permitted	Permitted	Permitted	Permitted	Forbidden	Permitted	Permitted	Permitted	Forbidden
Open Information in the public domain such as published research, marketing materials, policies, external website pages and other publicly released information	Permitted	Permitted	Permitted	Permitted	Permitted	Permitted	Permitted	Permitted	Permitted	Permitted	Permitted	Forbidden	Permitted

Truly anonymous - means data which does not relate to an identified or identifiable individual or data rendered anonymous in such a way that individuals are not (or are no longer) identifiable to anyone.

Permitted with auditable additional measures - means controls such as encryption, which have not been applied by the user; please contact your Information Governance lead in the first instance. If your Information Governance lead is unable to assist, then please contact its-research-consultants@qmul.ac.uk if your query is related to research data. If your query is related to non-research data, then please contact your Faculty Relationship Manager.

If you are unable to find a specific Type of Information, consult the Records Retention Schedule. If you are still in need of assistance, please contact information-security@qmul.ac.uk

14. Definitions

Term	Meaning
Information Asset	Where valuable information or data is captured and stored. This can be systems, physical paper, mobile devices and media such as DVDs, 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
SET	The Senior Executive Team (SET) 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
SFTP	Secure File Transfer Protocol

SCP	Secure Copy Protocol
RSync	A utility for efficiently transferring and synchronizing files between a computer and a storage drive and across networked computers
MFA	Multi-factor authentication (put in place to better secure access)