Handling Data & Information Breach			
Process Number:	**DG05-PR01**	Version Number:	**2.0**
Effective Date:	**14/01/2019**	Review Date:	**15/01/2021**

Author: Reviewers:	**Paul Smallcombe, Records & Information Compliance Manager** **David Pick, Network Security, IT Services** **Paul Smallcombe, Records & Information Compliance Manager** **Henrik Brogger, Head of IT Delivery, IT Services** **Kathy Whelan, IT Service Desk Manager, IT Services** **David Boakes, Assistant Director IT Operations & CISO** **Skender Osmani, Head of Client Devices, IT Services** **Richard Hughes, Customer Campus Support Manager Mile End** **Adam Thurston, Customer Campus Manager, Whitechapel** **Devin Singh, IT Service Desk Analyst**

Authorisation:	
Name / Position	**IT Lead team**
Signature	**IT Lead Team**
Date	**19/12/2019**

Revision History			
Version	Description	Author	Date
1.1	Minor revision following review	Paul Smallcombe	08/08/2014
1.2	Review the Process and update	Shelim Miah	19/09/2019
1.3	Feedback and comments	Shelim Miah	02/10/2019
1.4	Feedback and Comments	Madalyn Hardaker	04/11/2019
1.5	Title Change from Information Security Handling process	Shelim Miah	19.12.2019

Purpose and Objective:	
To define the procedures for which information security incidents need to be reported and how. An information security incident is any event that places any information held by Queen Mary University of London at risk of loss, unauthorised disclosure or unauthorised alteration, including destruction.	
Trigger:	Information security incident detected
Inputs:	Information Security Incident Log Register of Data Sets
Outputs:	Information Security Incident Log updated Remedial Actions Incident Report

References:
SOP DG05 – Information Security Incident Reporting SOP DG09 – Information Classification SOP DG27 – IT Security Incident Management WI DG-WI-27-01 IT Security Incident Management

Queen Mary University of London

Information Commissioner's Resources for Personal Data Breach Reporting

Process Steps

	Responsibility	Activity
1.	Person who discovers an incident (or other competent person)	**Immediate Containment and Recovery** When an information security incident is detected, ascertain whether the incident is still occurring. If so, steps must be taken immediately to minimise the effect of the breach, for example by shutting down a system, removing media, securing a physical area or equipment, alerting relevant staff. This action should be taken by someone who is competent to do so; if the person discovering the incident is not, then the QMUL Information Security Incident Team will determine who is when the incident has been reported.
2.	Person who discovers an incident	**Incident Reporting** The person who discovers or receives a report of an incident must inform their Local Information Security Manager or equivalent person who shall inform the head of their department. If the incident occurs or is discovered outside normal working hours, this should be as soon as is practicable. The incident must then be reported as soon as practicable to the QMUL Information Security Incident Team by emailing information-security@qmul.ac.uk or by telephoning 0207 882 7596 (internal 13 7596). The QMUL Information Security Incident Team shall consist of the QMUL Records & Information Compliance Manager, the Assistant Registrar, Council & Governance and the Academic Registrar and Council Secretary's nominee.
3.	QMUL Information Security Incident Team	An entry shall be made in the Incident Log, which is found at: Restricted\RIM Compliance\Information Security\Incidents. The data owner shall be notified.
4.	QMUL Information Security Incident Team	If it is determined that there is any IT information security aspect to the incident then the IT Security Team shall be informed by emailing it-security@qmul.ac.uk or by telephoning 020 7882 7079. Or contacting the IT Service Desk via Email: servicedesk@qmul.ac.uk In this case DG27-P01 shall subsequently be followed.
5.	QMUL Information Security Incident Team	The Local Information Security Manager shall be consulted (as will the IT Security Team if the incident is IT-related) and an Incident Manager assigned. This Incident Manager will normally be the QMUL Records & Information Compliance Manager or the Local Information Security Manager or suitable individual.
6.	Incident Manager (or other qualified person)	**Determine Incident Severity** In order to grade the severity of the incident (and decide on next steps), an assessment of the potential adverse effects must be carried out. This will need to include how many people are affected, the seriousness of any consequences and the likelihood of these happening. • What type of information is involved? • Is it protected e.g. with encryption?

		• What has happened to the information? • How many people have been or are likely to be affected? • What harm can come to any individuals? • Are there risks to safety, financial or reputational loss or to public health? • Are there any other wider consequences? Incidents must be graded as indicated in Appendix B.
7.	QMUL Information Security Incident Team	**Incident Management** For Grade 3 incidents, once immediate remedial action has been taken and the incident logged no further action will be required, unless it's indicative of an underlying problem or faulty system – e.g. if the same Grade 3 incident is recurrent there may be a bigger issue worth investigating. Update the Incident Log and close the incident.
8.	Incident Manager / QMUL Estates Security Service	For Grade 1 incidents where illegal activity is known or is believed to have occurred, or for Grade 1 or 2 incidents where there is a risk that illegal activity might occur in the future, it may be appropriate to contact the police. QMUL Estates Security Service will initiate the contact with the police as necessary. In any case, Grade 1 incidents will be escalated to the Academic Registrar and Council Secretary and other senior management as appropriate.
9.	Data owner and QMUL Information Security Incident Team	The Data Owner, and / or assigned member(s) of the QMUL Information Security Incident Team must quickly take appropriate steps to recover any losses and limit the damage which might include: a. Attempting to recover lost equipment b. Securing physical locations c. Contacting other relevant QMUL Departments, so that they are prepared for any potentially inappropriate enquiries 'phishing' for further information about the individuals whose data has been compromised. Consideration should be given to a global email. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual making the enquiry back. Whatever the outcome of the call, it should be reported immediately to the IT Security Team d. Contacting the Communications Office so that it can be prepared to handle any press enquiries e. Powering down or removing compromised equipment f. The use of back-ups to restore lost/damaged/stolen data g. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use h. If the data breach includes any entry codes or passwords, then these codes must be changed immediately, and the relevant agencies and members of staff informed i. If the incident concerns possession of information which a member of staff is not legally entitled to hold then the information must be destroyed or returned to its legitimate owner as soon as possible

10.	All staff	Longer-term measures might include: a. Change passwords and/or locks b. Modify access controls, issue keys to authorised personnel only c. Restore systems and assets d. Apply patches and updates, ensure firewalls and anti-virus are enabled e. Re-train staff and make them all security-aware
11.	Incident Manager	**Post Incident Investigation** In most cases the next stage would be for an assigned Investigator to fully look into the incident. The Incident Manager shall assume or appoint this role. S/he should ascertain what and whose data was involved, the potential and actual effect on Data Subjects and what further steps need to be taken to remedy the situation.
12.	Incident Manager	The investigation should consider: • The type of data, its sensitivity, what protections are in place (e.g. encryption), • What has happened to the data, • Whether the data could be put to an illegal or inappropriate use, • How many people are affected, • What type of people have been affected (the public, suppliers etc.) • Whether there are wider consequences such as whether it can be re-used (e.g. for fraudulent purposes). A clear record should be made of the nature of the incident and the actions taken in as much detail as possible in the Incident Log.
13.	Incident Manager	The investigation should be completed urgently and wherever possible within 24 hours of the incident being discovered / reported. A further review of the causes and recommendations for future improvements can be done once the matter has been resolved.
14.	QM Information Security Incident Team / Data Owner	**Notification** Some people and/or agencies may need to be notified as part of the initial containment and management. However, the decision will normally be made once an investigation has taken place. The QM Information Security Incident Team shall decide whether anyone should be notified of the breach and how. The Data Owner shall inform Data Subjects if appropriate. In the case of significant incidents involving personal data the Information Commissioner's Office (ICO) should be notified within 72hrs. The Barts Health Information Governance Team shall be notified if any BH NHS Trust data is impacted by contacting bartshealth.infogov@nhs.net. 'OfS (previously known as HEFCE) shall also be notified where appropriate by following QMUL's 'serious incident' procedure.

		Every incident should be considered on a case-by-case basis. The following points can be considered in deciding whether and how to notify: • Are there any legal or contractual requirements to notify? • Will notification help to prevent the unauthorised or unlawful use of personal data? • Could notification help the individual i.e. so they can act to mitigate the risks and impact? • If a large number of people are affected, or there are very serious consequences, the ICO should be notified. The ICO should only be notified if personal data is involved; guidance is available at : https://ico.org.uk/for-organisations/gdpr-resources/pdb/ • Consider the risks of over-notifying. Not every incident warrants it and may cause disproportionate enquiries and work • Decide whether to inform individuals by letter, email or via a website (or a combination) • The notification should include a description of how and when the incident occurred and what data was involved. Also include details of what has already been done to mitigate the risks posed and the effects. • When notifying individuals, give specific and clear advice on what they can do to protect themselves and what QMUL is willing to do to help them. Where possible Provide contact details of who they can reach out to with further questions. Update the Incident Log.
15.	QM Records & Information Compliance Manager	**Review and Evaluation** For Grade 1 and 2 incidents, once the initial aftermath of the incident is over, the QMUL Records & Information Compliance Manager shall fully review both the causes of the incident and the effectiveness of the response to it.
16.	Incident Manager	An incident report should be written and sent to the Records & Information Compliance Manager to include: • Description of events indicating specific timelines, personnel involved, • How it was discovered, • Activities leading up to the incident, • Impact on QMUL and other parties, • Decisions and actions taken, • Problems encountered, • Successful and unsuccessful activities, • Notifications required, • How notification was undertaken, • Steps taken for containment and remediation, • Recommendations for prevention, • Identification of policy or procedure gaps, results of post-incident review.

17.	Data Owner / QMUL Records & Information Compliance Manager	The Data Owner and/or the head of their department shall provide a response to the incident report and then the Records & Information Compliance Manager shall check that any remedy has been taken. This is not necessary for Grade 3 incidents. In the case of Grade 1 and 2 incidents the incident report will be communicated to senior management if they have not already been informed as part of any previous stage. The incident will then be closed.
18.	QMUL Information Security Incident Team	If systemic or ongoing problems are identified, then an action plan must be drawn up to remedy these. If the incident warrants a disciplinary investigation, the manager leading this should liaise with Human Resources for advice and guidance. If the law has been broken then legal proceedings may also result. Certain incidents, such as those involving fraud, may also have to be notified to QMUL's internal auditors. In any of these cases it will be necessary to collect evidence.

Appendix A – Fields of the Incident Log

1. Incident Number
2. Date of Incident (if known)
3. Discovered by
4. Email address
5. Date / Time of Discovery
6. Reported to Incident Team by
7. Date / Time Reported
8. Description of Information at risk (include data set references if available)
9. Where and How Held
10. Classification of Information
11. Owner of data
12. Which Department(s)
13. If third party involved (and details)
14. Description of Incident (how discovered, impact etc.)
15. Immediate Remedial Action Taken
16. Severity Grading
17. Investigator
18. Date appointed
19. Result of investigation
20. Is Notification required?
21. If yes, to which parties
22. Date(s) of Notification
23. Necessary to notify BLT NHS
24. Action plan

Appendix B – Incident Grades

Grade	Description
Grade 1	This is for illegal activities which must be notified to a law enforcement agency
Grade 2	This is for serious incidents which impact on a number of IT systems or users or Data Subjects
Grade 3	This is for low level/routine incidents where the impact is limited

Appendix C – Example Incidents and Assigned Grades

The following table lists example incidents and the grades that are likely to be assigned to each to assist with the grading process in step (6):

Description	Grade	Why?
A records storage room is found unlocked and it is clear that no information has been compromised	3	Unless in an area accessible to unauthorised individuals the impact is likely to be low or zero
A research folder with the names and addresses of a clinical trial's participants is taken offsite and misplaced	2	As this involves the breach of special category personal data, notification would be essential and could lead to reputational damage to QMUL
A spreadsheet of (<100, >100) students' examination marks is mistakenly emailed to an external party	2 or 3	Depending on the number of individuals affected this would reveal personal data but the impact is likely to be limited unless a complaint is made to the Information Commissioner's Office that the breach has caused damage/distress to one or more students
A fire destroys a large number of records	2	Information loss could have a serious impact on the ability of QMUL to fulfil certain functions if there are no backups
A member of staff is found to have sold personal data to an organisation for use in marketing	1	This is an offence under Section 170 of the Data Protection Act 2018. This would also lead to internal disciplinary action

Queen Mary University of London

Queen Mary University of London

Appendix D - Information Security Incident Report Form

Incident Number (for internal use)
IS

Fill in as much information as possible and then send this form to the Information Security Incident Team information-security@qmul.ac.uk

1. Date of Incident (if known)

2. Discovered by	
Name	
Position	
Phone	
Email	

3. Date and Time of Discovery

4. Reported by	
Name	
Position	
Phone	
Email	

5. Date and Time Reported

6. Description of Data at risk (include data set reference if available)

7. Classification of Information (see SOP DG09; tick one option)	
Highly Confidential	
Confidential	
Restricted	
Protect	

8. Owner of data
Department (include where and how the data is/was held and details of any other departments which may be impacted)

9. a) If yes to previous question, specify here

10. Description of incident (include as much detail as possible including how discovered, impact etc.)

11. Immediate remedial action taken

Form Submission:
Email to information-security@qmul.ac.uk

(The following boxes are for internal use)

11. Severity Grading (tick one option)	
Grade 1: illegal incidents	
Grade 2: serious incidents	
Grade 3: routine incidents	

12. Investigator	
Name	
Contact details	
Date appointed	

13. Result of investigation

14. Is Notification required? If 'no' go to 17.
14. a) If yes, to which parties?

15. Date(s) of Notification

16. Necessary to notify BLT NHS

17. Action Plan to remedy

Appendix E – Process Flow