Standard Operating Procedures (SOP) for:			
Information Security Incident Reporting			
SOP Number:	**DG05**	Version Number:	**1.1**
Effective Date:	**07 Dec 2015**	Review Date:	**07/12/18**

Author: Reviewer:	**David Pick, IT Services Security** **Paul Smallcombe, Records & Information Compliance Manager**

Authorisation:	
Name / Position	**IT Services Lead team**
Signature	**C Day**
Date	**23 November 2015**
Name / Position	**Paul Smallcombe, Records & Information Compliance Manager**
Signature	**Paul Smallcombe**
Date	**29 May 2015**

Accountability:	
Position	Line Managers
Responsibility:	
Position	Directors/ Heads of Department Records & Information Compliance Manager Information Owners

Revision History			
Version	Description	Author	Date
1	Initial version.	David Pick	12/04/2010
1	Annual review- No change	Paul Smallcombe	04/03/2014
1.1	Annual Review - Minor updates	Paul Smallcombe	29/05/2015

Purpose and Objective:
To ensure that information security incidents are handled in accordance with industry best practice. Information security incidents may involve the loss or theft of physical and/or electronic information assets or damage to these. The process for managing IT security incidents is described in SOP DG27 – IT Security Incident Management.

References:
SOP DG09 – Information Classification SOP DG13 – Records Management SOP DG27 – IT Security Incident Management

SOP Text

	Responsibility	Activity
1.	Directors/ Heads of Department	Each Director/ Head of Department shall inform the Queen Mary Records & Information Compliance Manager of the existence of any data sets within their areas of responsibility containing Confidential or Restricted information as defined by SOP DG09 –

		Information Classification.
2.	QM Records & Information Compliance Manager	Queen Mary shall maintain a register of data sets held that contain Confidential or Restricted information together with the name and role of the data owner and details of the organisation (internal or external) they work for. Refer to SOP DG13 – Records Management.
3.	QM Records & Information Compliance Manager	Queen Mary shall maintain a log of all incidents that may impinge on any aspect of data security including, but not limited to, the confidentiality and integrity of the data. Refer to SOP DG13 – Records Management.
4.	QM Records & Information Compliance Manager	Queen Mary shall publish guidance about which types of data set or incident needs to be recorded in these registers or logs. Refer to SOP DG09 – Information Classification. Queen Mary shall publicise this guidance periodically to all members of Queen Mary.
5.	Line Manager	When an information security incident is detected the appropriate line manager shall assign a member of staff to act as an Incident Manager. An information security incident could be triggered as a result of a breach of physical security or a staff member reporting the loss or theft of information, or the discovery of information that Queen Mary is not legally entitled to hold.
6.	Incident Manager	The Incident Manager shall determine if any computer equipment might have been accessed and, if so, report it as a possible breach of IT security to the IT Security Team, as per SOP DG27 – IT Security Incident Management. The Incident Manager shall make a list of all non-computer-based information possibly placed at risk and report this to the QM Records & Information Compliance Manager.
7.	QM Records & Information Compliance Manager	The QM Records & Information Compliance Manager shall make entries in the log of incidents. If any of the data sets are in the register of Confidential or Restricted data the data owner shall be notified (see item 9).
8.	Any person investigating a breach of IT Security QM Records & Information Compliance Manager	Where a breach of IT security is detected it shall be investigated by a technically competent person. The investigator shall make a list of all computer-based information possibly placed at risk and report this to the QM Records & Information Compliance Manager. The QM Records & Information Compliance Manager shall make entries in the log of incidents. If any of the data sets are in the register of Confidential or Restricted data the data owner shall be notified (see item 9).
9.	Owners of Confidential or Restricted Information	Whenever any data owner listed in the register of Confidential or Restricted information is notified of a possible breach of security, they shall determine the nature of the risk and take remedial action. This may include notifying all individual persons identified in the data set of the possible breach, what information was at what risk, and what action is being taken. If the data owner is Barts Health NHS Trust (BH) then the BH Information Governance Team shall be informed.

10.	All Members of Queen Mary	Any disclosure of computer account credentials shall be regarded as a breach of IT security and shall be handled as per SOP DG27 – IT Security Incident Management.
11.	QM Records & Information Compliance Manager	The contents of the incident log shall be reviewed periodically, and in any case at least annually, and a report made to the Information Governance Group.
12.	QM Records & Information Compliance Manager	Any incident deemed to be serious by the QM Records & Information Compliance Manager shall be escalated to the Queen Mary Senior Executive immediately, who will provide a report to the Audit and Risk Committee.
13.	QM Records & Information Compliance Manager Owners of Confidential or Restricted Information	If a risk to Confidential or Restricted information is identified it shall be reported to the QM Records & Information Compliance Manager who shall determine from the register the data owner responsible for the information at risk. The data owner shall assign an Incident Manager who shall determine the remedial action that must be taken.
14.	QM Records & Information Compliance Manager Owners of Confidential or Restricted Information	The QM Records & Information Compliance Manager shall arrange periodic reviews, at least annually, of the information security requirements of each Confidential or Restricted data set in the register. These reviews shall check current security procedures for that data set and any changes in procedures, legislation or regulatory regimes that may apply.