Standard Operating Procedures (SOP) for:			
Handling Information			
SOP Number:	**DG15**	Version Number:	**1.2**
Effective Date:	**07 Dec 2015**	Review Date:	**29/05/2018**

Author: Reviewer:	**Benjamin Roberts, Dental Electronic Resources Manager** **Paul Smallcombe, Records & Information Compliance Manager** **Ian Douglas, Head of IT Security**

Authorisation:	
Name / Position	**IT Services Lead Team**
Signature	**C Day, Director of IT Services**
Date	**23 November 2015**
Name / Position	**Paul Smallcombe, Records & Information Compliance Manager**
Signature	**Paul Smallcombe**
Date	**23 July 2015**

Accountability:	
Position	Line Managers
Responsibility:	
Position	Directors/ Heads of Department Information Security Managers Information Owners

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

Purpose and Objective:
To ensure that information in all formats and media is handled appropriately such that this information is protected from unauthorized disclosure or misuse according to its classification as per Appendix A of SOP DG09 – Information Classification. Measures should be taken appropriate to the category of information.

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

SOP Text

	Responsibility	Activity
1.	User	Information shall be stored as per SOP DG14 – Storage of Information.
2.	User	Media shall be labelled to indicate the classification level as per SOP DG09 – Information Classification.
3.	User / IT Services	Information shall only be transferred across information networks when the required confidentiality and integrity of the information can be assured.
4.	User / IT Services	Confidential or Restricted information transmitted, either by computer network or physically in the form of removable media or a mobile computing device, shall be encrypted. Guidance regarding the encryption of information is provided in SOP DG12 – Cryptographic Controls.
5.	User / Information Security Manager	Hard copies of Confidential or Restricted information shall be handled appropriately. Removal off site shall be authorised by an appropriate manager and a record kept of this authorisation. Prior to authorisation, a risk assessment based on the criticality of the information asset shall be carried out.
6.	Information Owner	Physical media containing Confidential or Restricted information in transit shall be protected as follows: a) reliable transport or couriers should be used; b) a list of authorised couriers shall be agreed with management; c) couriers shall be identified; d) packaging shall protect the contents from any physical damage; e) controls shall protect information using the following methods - use of locked containers - delivery by hand - tamper-evident-packing - in exceptional cases, the consignment shall be split into more than one delivery and dispatched by different routes.
7.	Information Owner	A record of the authorised recipients of Confidential or Restricted information shall be maintained.
8.	Information Owner	The record of authorised recipients of Confidential or Restricted information shall be reviewed at regular intervals. The minimum review period shall be a year.
9.	Information Owner	The distribution of Confidential or Restricted information shall be minimised.
10.	Information Owner	Third parties in receipt of information shall maintain the required confidentiality and integrity of that information asset. Relevant identity information for the third party shall be verified prior to

		the dispatch of any information asset. The dispatch or removal of information shall be authorised by its owner.
11.	Information Owner	Information owners shall ensure that appropriate backup, recovery and archival procedures are in place. See SOP DG26 – System Backup and Recovery.
12.	Information Owner / QM Records & Information Compliance Manager	Any information security incident, for example where handling leads to leak or loss of information, shall be dealt with as per SOP DG05 – Information Security Incident Reporting.
13.	IT Services	Due care shall 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 The QM IT Security Team shall provide advice as necessary to any person engaged or considering such an intrusion. The QM IT Security Team shall 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.
14.	IT Services	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 NB: The RIPA and Lawful Business Practice Regulations 2000 do allow for legitimate interceptions of communications by organisations on their private computer and telecommunications networks - in other words, they provide 'lawful authority'.