Standard Operating Procedures (SOP) for:			
Cryptographic Controls			
SOP Number:	**DG12**	Version Number:	**1.1**
Effective Date:	**07 Dec 2015**	Review Date:	**21/07/2018**

Author: Reviewer:	**Benjamin Roberts, Dental Electronic Resources 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**

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

Revision History			
Version	Description	Author	Date
1	Initial version.	Benjamin Roberts	21/04/2010
1	Annual Review	Ian Douglas	23/07/2014
1.1	Update paragraph 13	Ian Douglas	29/05/2015

Purpose and Objective:
To protect the confidentiality, authenticity or integrity of information by cryptographic controls.

References:
SOP DG09 – Information Classification SOP DG19 – Remote Access

SOP Text

	Responsibility	Activity
1.	Business Manager of Organisational Unit	Each organisational unit of the College shall have an Information Security Manager. One responsibility of the Information Security Manager is to advise members of that organisational unit about the use of encryption technology.
2.	Information Security Manager	The Information Security Manager shall identify the appropriate level of encryption protection in a given security situation.
3.	Information Security Manager	The Information Security Manager shall ensure that secret keys are securely recorded and stored so that encrypted data can be accessed by authorised persons if a key's owner is unavailable.

4.	User	Where secret key encryption is used it is the responsibility of the user, or group of users, to keep the key secret. Secret keys shall only be given to users who are authorised to have access to the information.
5.	User	Where public key encryption is used users shall not share their private key.
6.	User	Secret and private keys shall only be stored in an unencrypted form if there are both pressing operational requirements that dictate this (for example the need to allow equipment to restart unattended) and if increased care is taken to protect access to the storage medium.
7.	User	Where a secret key has been compromised, the information shall be decrypted using the compromised key and immediately encrypted using a new key. All on-line data encrypted using the old key shall be re-encrypted using the new key. Off-line encrypted data held securely shall not be decrypted and re-encrypted.
8.	IT Services or Head of Department/ Director of Institute	Arrangements shall be made to ensure that any encrypted copies of business critical information must be recoverable after a disaster. Possible techniques may include, but are not limited to, the use of protected backups of the keys or the use of a key-escrow technique.
9.	User	Mobile devices (e.g. laptops, mobile phones, PDAs, etc.) shall all be encrypted. Removable media (e.g. USB sticks, DVDs, etc.) containing Confidential or Restricted data shall be encrypted.
10.	User	Standalone computers, and networked PCs storing data locally, that contain Confidential or Restricted data (see SOP DG09 - Information Classification) shall be encrypted.
11.	IT Services or Head of Department/Director of Institute responsible for the Information Asset	Encryption shall be used for remote access connections to College information assets. Refer to SOP DG19 - Remote Access.
12.	User	Where a member of staff is uncertain whether a cryptographic solution is appropriate this decision shall be referred to the Information Security Manager.
13.	User / Information Security Manager	Information shall be encrypted using the current best practise encryption technique, for advice contact the QM IT Security Team.