Standard Operating Procedures (SOP) for:

**Cryptographic Controls**

<table>
<thead>
<tr>
<th>SOP Number:</th>
<th>DG12</th>
<th>Version Number:</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
<td>15 July 2014</td>
<td>Review Date:</td>
<td>23/07/2015</td>
</tr>
</tbody>
</table>

**Author:**
Benjamin Roberts, Dental Electronic Resources Manager
Ian Douglas, Head of IT Security

**Authorisation:**
Name / Position: Chris Day, Acting Director of IT Services
Signature: C Day
Date: 15 July 2014

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

**Revision History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Author</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initial version.</td>
<td>Benjamin Roberts</td>
<td>21/04/2010</td>
</tr>
<tr>
<td>1</td>
<td>Annual Review</td>
<td>Ian Douglas</td>
<td>23/07/2014</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Business Manager of Organisational Unit</td>
<td>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.</td>
</tr>
<tr>
<td>2. Information Security Manager</td>
<td>The Information Security Manager shall identify the appropriate level of encryption protection in a given security situation.</td>
</tr>
<tr>
<td>3. Information Security Manager</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 only be used to store Confidential or Restricted data (see SOP DG09 – Information Classification) if the device supports encryption and the data is encrypted to the level required by this procedure. Removable media (e.g. USB sticks, DVDs, etc.) containing Confidential or Restricted data shall be encrypted.

10. **User**
    Stand alone 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 Advanced Encryption Standard (AES) – 256 or stronger technique as advised by the QM IT Security Team.