Standard Operating Procedures (SOP) for:			
Storage of Information			
SOP Number:	**DG14**	Version Number:	**1.2**
Effective Date:	**07 Dec 2015**	Review Date:	**15/05/2018**

Author: Reviewer:	**Benjamin Roberts, Dental Electronic Resources Manager** **Paul Smallcombe, Records & Information Compliance Manager**

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	**Pau Smallcombe**
Date	**15 May 2015**

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

Revision History			
Version	Description	Author	Date
1	Initial version.	Benjamin Roberts	22/04/2010
1.1	Annual Review – Minor wording changes	Paul Smallcombe	15/05/2014
1.2	Annual Review – Minor wording amendments	Paul Smallcombe	29/05/2015

Purpose and Objective:
To ensure that information in all formats and media is stored securely 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 DG09 – Information Classification SOP DG11 – System Access Controls SOP DG12 – Cryptographic Controls SOP DG13 – Records Management

SOP Text

	Responsibility	Activity
1.	User	Information shall be stored such that it is secured against loss, damage and unauthorised access or modification.

2.	IT Services / Departments Operating Computer Systems	Information shall be accessible to authorised users at times when they require it.
3.	User / IT Services / Departments Operating Computer Systems	All Confidential and Restricted information shall be access controlled in accordance with SOP DG11 – System Access Controls. This applies to information in all forms.
4.	User	Confidential and Restricted information shall not be stored on mobile devices or removable media (e.g. USB sticks, laptop computers, mobile phones etc.) and non-mobile storage not in a physical secure area (i.e. NAS Device, Server attached storage etc.) unless it is encrypted. See SOP DG12 – Cryptographic Controls.
5.	IT Services / Departments Operating Computer Systems	Information shall be regularly backed up.
6.	Estates / IT Services / Departments Operating Computer Systems	Information shall be stored on or in equipment and/or in locations that are sited or protected to reduce the risks from environmental threats and hazards and opportunities for unauthorised access or other damage.
7.	Estates / IT Services / Departments Operating Computer Systems	Information shall be stored on or in equipment protected from power failures and other disruptions caused by failures of supporting utilities.
8.	User / IT Services / Departments Operating Computer Systems	Electronic information shall be checked every five years or when there is a system upgrade, whichever is soonest, to ensure that it can still be accessed.