

Standard Operating Procedures (SOP) for:			
<b>Disposal of Information</b>			
SOP Number:	<b>DG16</b>	Version Number:	<b>1.1</b>
Effective Date:	<b>07 Dec 2015</b>	Review Date:	<b>29/05/2018</b>

Author:	<b>Benjamin Roberts, Dental Electronic Resources Manager</b>
Reviewer:	<b>Paul Smallcombe, Records &amp; Information Compliance Manager</b>

Authorisation:	
Name / Position	<b>IT Services Lead Team</b>
Signature	<b>C Day, Director of IT Services</b>
Date	<b>23 November 2015</b>
Name / Position	<b>Paul Smallcombe, Records &amp; Information Compliance Manager</b>
Signature	<b>Paul Smallcombe</b>
Date	<b>29 May 2015</b>

Accountability:	
Position	Line Managers
Responsibility:	
Position	Information Owners Information Security Managers QM Records & Information Compliance Manager

Revision History			
Version	Description	Author	Date
1	Initial version.	Benjamin Roberts	22/04/2010
1.1	Annual Review – Small changes	Paul Smallcombe	15/05/2014
1.1	Annual Review – No Change	Paul Smallcombe	29/05/2015

Purpose and Objective:	
To ensure the appropriate disposal of information, or computer systems or hardware containing or having contained information, according to its classification as per Appendix A of SOP DG09 – Information Classification. Measures should be taken appropriate to the category of information in all formats and media.	

References:	
SOP DG09 – Information Classification SOP DG10 – IT Equipment Disposal	

SOP Text
----------

	Responsibility	Activity
1.	Information Owner	All items of equipment containing storage media shall be checked to ensure that any Confidential or Restricted information, as

		defined in SOP DG09 – Information Classification, has been removed or securely overwritten prior to disposal.
2.	Information Owner	<b>Disposal of Confidential or Restricted physical information</b> Paper records or other physical records, such as film, shall be destroyed by shredding (via use of confidential waste bins where available) or otherwise physically destroyed such that the information cannot be recovered.
3.	Information Owner  QM IT Security Team  Information Security Manager	<b>Disposal of Confidential or Restricted electronic information</b> When computer data is to be destroyed formatting a disk drive is not adequate. To ensure secure deletion, a product that overwrites data many times shall be used, such that the information cannot be recovered. The QM IT Security Team shall provide guidance and advice about the use of such products.  Media and devices holding electronic data including, but not limited to CDs, DVDs, tapes, diskettes, flash memory devices, and PDAs, shall be either physically destroyed or disposed of via a company that specialises in secure data destruction, who will collect hardware and ensure all data thereon is destroyed. See SOP DG10 – IT Equipment Disposal. IT Services shall provide departments with details of suitable disposal companies on request.  The local Information Security Manager shall advise the most appropriate course of action.
4.	Information Owner	Where a third party performs any destruction on behalf of the College this SOP shall be followed and the third party shall provide a certificate confirming destruction. Where the Confidential or Restricted information consists of personal information, the third party shall be contracted under the terms of a data processor agreement.
5.	Information Owner / Information Security Manager	All damaged devices containing information shall be subject to a risk assessment prior to being removed off site for repair.
6.	Information Owner / QM Records & Information Compliance Manager	A record shall be kept of all information and media which has been disposed of.