Policy on Secure Disposal of IT Equipment and Information v1.0

Organisation	Oxford Brookes University
Title	Policy on Secure Disposal of IT Equipment and Information
Creator	Information Security Working Group
Approvals Required	1. Information Security Working Group 2. CIO 3. Executive Board
Version	Version 1.0
Owner	Executive Board
Subject	The formal University policy on the secure disposal of IT equipment and information
Rights	Public
Review date and Responsibility	Annually by Information Security Working Group

1. **Introduction**

The University holds and processes a large amount of information and is required to protect that information in line with relevant legislation and in conformity with University regulations and policies such as the Information Security Policy[link], the Data Protection Policy[link] and the Records Management Policy[link]. This policy sets out the requirements for staff on the secure disposal of the University's IT equipment and information.

2. **Definitions**

2.1 Secure Disposal

Secure disposal means the process and outcome by which information including information held on IT equipment is irretrievably destroyed in a manner which maintains the security of the equipment and information during the process and up to the point of irretrievable destruction.

2.2 IT Equipment

IT equipment means all equipment purchased by or provided by the University to store or process information including but not necessarily limited to desktop computers, servers, printers, copiers, laptops, tablet computers, electronic notebooks, mobile telephones, digital recorders, cameras, USB sticks, DVDs, CDs and other portable devices and removable media.

2.3 Information

2.3.1 Information means all information and data held or recorded electronically on IT equipment or manually held or recorded on paper.

2.3.2 For the purpose of this policy, the information held by the University can be divided into two categories: non-sensitive; and sensitive information. Sensitive information comprises: all personal information and all confidential information, the loss of which would, or would be likely to, cause damage or distress to individuals or to the University.

2.3.3 The default category is that all information is deemed to be sensitive unless specifically identified as otherwise.

3. **Responsibilities**

3.1 It is the responsibility of all University staff to ensure that the information held by the University is disposed of appropriately and that all sensitive information is disposed of securely.

3.2 Responsibility for this policy resides with the University's Executive Board. Implementation of this policy is managed through the University's Information Security Working Group which reports to the Chief Information Officer.

4. **Statement of Policy**

4.1 This policy on disposal covers all data or information held by the University whether held digitally or electronically on IT equipment or as manual records held on paper or in hard copy.

4.2 It is the University's policy to ensure that all information held by the University is disposed of appropriately, in conformity with the University's legal obligations and in accordance with the University's regulations[link] and Records Management policy[link].

4.3 In particular it is the University's policy to ensure that all sensitive information which requires disposal is disposed of securely.

4.4 Where information is held on IT equipment, it is the policy of the University that such equipment will be assumed to hold sensitive information and that all information residing on such equipment must be disposed of securely.

4.5 The University supports policies which promote sustainability and take account of environmental impact. The University will therefore support recycling or sustainable redeployment in the disposal of IT equipment as long as information held on the equipment is irretrievably and securely destroyed prior to the the disposal of the equipment.

4.6 WEEE: IT equipment must also be disposed of in line with the EU Waste Electrical and Electronic Equipment (WEEE) Directive and the UK Waste Electrical and Electronic Equipment Regulations 2006.
[Link www.brookes.ac.uk/Documents/About/Sustainability/en103w2/]

4.7 Copyright: software must be disposed of in line with copyright legislation and software licensing provisions.

5. **Policy Principles**

5.1 Hard copy

5.1.1 Information and data held in paper or hard copy which contain sensitive information shall be irretrievably destroyed in a way in which the information cannot be reconstituted, by shredding, pulping or incineration.

5.1.2 The process leading to and the process of shredding, pulping or incinerating such information shall be carried out securely.

5.1.3 Where the shredding or incineration are carried out on behalf of the University by a third party, there shall be a contract with that third party which appropriately evidences:

a) that party's obligations to keep that data confidential and;

b) that party's responsibility under the Data Protection Act 1998 for the secure disposal of the data.

5.1.4 Where hard copy information is stored externally by a third party data storage contractor, the contract shall ensure secure disposal of the data at a time which conforms with the University's Retention Schedule[link].

5.2 IT Equipment

5.2.1 Since the policy default is that all IT equipment which stores or processes data will be deemed to hold sensitive data, then all such IT equipment will undergo appropriate physical destruction or an appropriate data overwrite procedure which irretrievably destroys any data or information held on that equipment.

5.2.2 Where an overwrite procedure fails to destroy the information irretrievably, the equipment shall be physically destroyed to the extent that the information contained in it is also irretrievably destroyed.

5.2.3 For the avoidance of doubt, removable digital media including but not limited to CDs, DVDs, USB drives, where the default is that they contain sensitive data, shall, if not successfully overwritten, be physically destroyed to the extent that all data contained in the media are irretrievable.

5.2.4 All IT equipment awaiting disposal must be stored and handled securely.

5.2.5 Where the overwriting procedure and/or physical destruction of IT equipment are carried out on behalf of the University by a third party, there shall be a contract with that third party which appropriately evidences: that party's obligations to keep that data confidential and; that party's responsibility under the Data Protection Act 1998 for the secure disposal of the data.

5.2.6 In any case where IT equipment is to be passed on by the University for re-use, those staff involved in the sale or transfer of the equipment shall ensure that any information on the equipment has been irretrievably destroyed and that any other appropriate issues, including, but not limited to, the safety of the equipment are satisfactorily addressed.

5.2.7 Photocopiers and printers used or owned by the University may have a data storage capacity. Where such IT equipment contains information or data, the disposal of such equipment must have due regard to this policy.

5.3 Online Data

5.3.1 The University has a contract with Google for the use of its Google Apps for Education. This enables University staff to take advantage of the features provided for data storage of emails and documents. The University does not sanction the use of external online (cloud) services for University data where there is no contract in place.

5.3.2 Data held in the University's Google applications or other authorised online storage applications should be destroyed to the extent possible by using the delete facilities provided.

6 **Record of Destruction**

6.1 Any third party contracted to dispose of sensitive hard copy information shall certify the irretrievable destruction of the information.

6.2 University staff who have responsibility for the information which is disposed of shall ensure that the disposal conforms with the University's Records Management policy[link] and Retention Schedule[link] and that, where necessary, a record is kept documenting the disposal.

6.3 Where the disposal involves the disposal of IT equipment, the University shall keep a record of the asset number of the equipment which has been disposed of along with a record of the process by which the information stored on the equipment has been irretrievably destroyed.

7 **Reporting**

7.1 All staff, students and other users of information should report immediately to the Service Desk via the Servicedesk portal https://service.brookes.ac.uk or by telephone (tel. ext. 3311) any observed or suspected incidents where sensitive information has or may have been insecurely disposed of.

8 **Advice and Assistance**

8.1 Advice on the implementation of this policy can be obtained from the University Information Compliance Officer (tel. ext. 4354: email address info.sec.@brookes.ac.uk) and the University Records Manager (tel. ext. 4046: email address dept_ric.addressbook@brookes.ac.uk)

8. 2 Advice on the disposal of IT equipment can be obtained from the University's IT department, OBIS, by contacting the Service Desk on tel. ext 3311 or via the Servicedesk portal https://service.brookes.ac.uk

9 Guidelines

9.1 Hard Copy

9.1.1 Staff holding University data in hard copy should routinely dispose of the data when it is no longer required to be held for legal or contractual purposes or is no longer necessary for the business purpose for which it was originally created or held. In determining whether and when the data should be disposed of, staff should consult the University's Retention Schedule

obis.brookes.ac.uk/records/Retention%20Schedule%201c.doc

Further information can be obtained from the University Records Manager.

9.1.2 It is good practice to shred, pulp or incinerate all University data which requires destruction. Where hard copy waste is sensitive data (as defined in 2.3.2) it should always be securely and irretrievably destroyed by shredding, pulping or incineration. In order to ensure the secure and irretrievable destruction of hard copy, staff are required to use the service provided by the University's selected contractor for the destruction of confidential waste.

9.1.3 Confidential waste bags for information requiring secure destruction can be obtained from Campus Services which will collect the bags when they are ready for disposal. Bags which contain confidential waste should be sealed and kept secure until collected by Campus Services.

9.1.4 Confidential waste bags awaiting collection or further processing should not be left in public areas or areas where they can be accessed by unauthorised staff.

9.1.5 Where sensitive data are stored under contract externally, staff responsible for the contract should ensure the contract includes secure, certificated destruction of the data in accordance with the appropriate retention period. External storage and destruction of University data should not be arranged without reference to the University Records Manager.

9.1.6 Where staff consider a document is of sufficient historic importance to be retained by the University, they should consult the University Archivist.

9.2 IT Equipment

9.2.1 Staff holding University data on IT equipment should routinely dispose of the data when it is no longer required to be held for legal or contractual purposes or is no longer necessary for the business purpose for which it was originally created or held. In determining whether and when the data should be disposed of, staff should consult the University's Retention Schedule [link obis.brookes.ac.uk/records/Retention%20Schedule%201c.doc].

Further information can be obtained from the University Records Manager (tel. ext. 4046: email address dept_ric.addressbook@brookes.ac.uk)

9.2.2 Where a decision has been made that data held on IT devices or media should not be retained, the files containing the data should be deleted from those devices. Deletion involves putting the information "beyond use" by the user of the device or media. Data held in a recycling "bin" on the device or data which can easily be recovered by the user are not regarded as being "beyond use" and may still be subject to discovery and disclosure under information law (Freedom of Information, Subject Access Request) or litigation.

9.2.3 Staff shall never dispose of University IT equipment (devices or media) without taking steps to ensure the irretrievable deletion of data held on the equipment.

9.2.4 Electronic or digital data which have been put "beyond use" by users may still be reconstituted by IT specialists or by forensic computer analysts. This means that when IT equipment (devices or media) are disposed of, the data should be

- irretrievably destroyed by being overwritten in accordance with the appropriate industry standard, or
- the hard disc containing the data within the equipment or the media containing the data (e.g. CD, USB stick) should be physically destroyed.

The University has some shredding machines available which can destroy CDs and DVDs as well as shred hard copy.

9.2.5 Staff requiring the disposal of IT equipment which holds or may hold University data should contact the Service Desk via the Servicedesk portal https://service.brookes.ac.uk (tel ext. 3311) to arrange for the disposal.

9.2.6 Staff should also be mindful that University mobile telephones contain data which will need to be extracted or deleted from the device before the device is disposed of. The telephone should be returned to the Service Desk should be contacted to initiate the secure return and disposal of the device.

9.2.7 While the University supports the recycling or sustainable redeployment of IT equipment, University staff shall not arrange for such a process without consulting the OBIS Client Device Support Manager contacted via the service desk via the Servicedesk portal https://service.brookes.ac.uk (tel. ext. 3311), obtaining appropriate authority from OBIS for the proposed recycling and ensuring that any data held on the equipment are securely and irretrievably destroyed.

9.2.8 Where University staff are leasing equipment (such as multi-functional copiers), staff responsible for the contracts should ensure that the leasing contract certifies the secure disposal of any University data held on the devices during the period of lease.

9.2.9 When disposing of IT equipment, staff must be mindful of the WEEE regulations. [Link http://www.brookes.ac.uk/about/sustainability/docs/en103w2.pdf]

9.3 Online data

9.3.1 Staff using the delete facility provided by Google in the University's online Google applications should be aware that the deleted material will be held for 30 days in their online "bin". Such data will not be regarded as "beyond use" until it has been further deleted from the "bin".

9.3.2 Online data held in Google accounts provided to staff by the University for the purpose of their employment are not automatically deleted when staff leave the University. These accounts are deactivated and access to the data retained for any necessary business purpose. Prior to leaving the University, staff should, wherever possible, ensure the appropriate management and handover of the University data in their accounts, deleting from their accounts data which are no longer required by the University.