IT Asset Secure Disposal Policy

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins

Chief Information Security officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	22/08/2016
V 0.2	Andrew Clarke	Formatting changes	02/02/2017
V 0.3	Andrew Clarke	Appendix A record retention	22/02/2017
V 0.4	Andrew Clarke	Process Flowcharts	27/07/2017
V 1.0	Andrew Clarke	Approved InfoSub Committee	26/01/2018
V 1.1	Andrew Clarke	Reformatting – removal of processes, adoption of Procurement Disposal of IT Equipment Policy	23/01/2020
	Andrew Clarke	Annual Review	08/06/2020

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

Owner: Michael Jenkins	Chief Information Security Officer
Signature: MGJ	Date: 26 Jan 2018
Approver: Pekka Kahkipuro	Chief Information Officer
Signature: PK	Date: 26 Jan 2018
Distribution:	

This document requires the approval from BUL as defined in the ISMS Compliance document.

Contents

1. About this document

1.0 Background

This document describes the policy for the disposal of University Confidential, and Protect classified assets which are the responsibility of Brunel University. This policy is part of the library of policy and procedure documents known as the Information Security Management System (ISMS), which in turn are a constituent part of the Risk Management Accreditation Document Set (RMADS).

Information and IT equipment are vital assets to any organisation, and this is especially so in the University which is a knowledge-driven organisation. Virtually all of our activities involve creating or handling information in one form or another via the IS equipment we use. The Asset Secure Disposal Policy and its associated processes are concerned with managing the secure disposal of IS equipment assets which are owned by the University and are no longer required.

1.1 Intended Audience

This document is aimed at Brunel University staff and its third party contractors responsible for the sanitisation, decommissioning or disposal of assets holding University Confidential and Protect marked data belonging to the Brunel University.

1.2 Objectives of This Policy

All staff/student(s) of the University who use information assets have a responsibility to handle them appropriately and in accordance with their classification.

Information Classification Policy

University information assets should be made available to all who have a legitimate need for them.

The integrity of information assets must be maintained at all times..

- To define the responsibilities of individuals for the secure disposal of University Assets;
- To provide a rigorous and consistent process to ensure University Assets which are deemed “end of life” or to be recycled, are securely wiped before being redistributed or leaving the University premises e.g. PCs, laptops and other devices that process and store University data;
- To provide advice on the appropriate methods of destruction of physical media;

- To ensure information assets stored via University IT equipment is sufficiently backed up, copied and/or removed prior to being disposed of;
- To ensure an auditable trail of disposal/destruction is evidenced;

1.3 Output - Data Erasure Reporting

A summary of reports will be collated and provided yearly to ensure an overview of the secure disposal process.

1.4 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Site Services Manager	• Is responsible for the University's soft services contracts including waste management and recycling for paper and media.
Head Of Archives And Records Management - Governance, Information and Legal Office	• Is responsible for the University Retention and Disposal Schedules Archives and Records Management.
Cyber & Information Security Manager	• Is responsible for maintaining the Process and to ensure that the Process continues best practice and ensuring compliance with legislative and regulatory requirements.
IS Procurement Manager	• Is responsible for ensuring that contracts with third parties engaged in secure disposal of University assets comply with this Process. • Is responsible for ensuring that assets are decommissioned and disposed of in compliance with this Process. • Is responsible for ensuring that asset disposal records, certificates and reports are maintained. • Is responsible for ensuring that University assets for disposal are retained on campus in a secure manner until collection for disposal.
Head of Customer Services - PC Support	• Is responsible for ensuring collection of assets for re-use and disposal and for secure wiping of hard drives to the agreed sanitisation level.
All employees – “Owner/User”	• Any user of University information assets (including mobile phones, laptops and/or other peripherals) may have specific custodianship responsibilities identified in their user agreements and have a responsibility to adhere to this Process

1.5 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001.

University ISMS Control Number	SOA – Number A8 – Asset Management SOA – Number A11 – Physical & Environmental Security
ISO 27001 Conformance Control	Information Classification Objective A.8.3.2 – Disposal of media A.11.2.7 - Secure disposal or reuse of equipment

1.6 File reference(s)

SPF – Security Policy Framework v5.0 dated April 2014

HMG Information Assurance Standard No. 5 v4.0 dated April 2011

HMG Information Assurance Standard No. 4 v5.0 dated April 2011

University Records Management Policy

Records Retention and Disposal Policy and Schedules

University Archive Policy

1.7 Acceptance criteria

Ref	Title	Criteria
1	Asset tracking	All assets earmarked for removal have been successfully tracked from desk to disposal with an end-to-end history.
2	Data Security	No End of Life asset has residual University Confidential or Protect marked data remaining at any point of leaving the University.
3	Disposal	All assets are either refurbished or disposed of within WEEE regulations with 0% non-biodegradable landfill footprint.
4	Reporting	Every disposed assets data sanitisation, removal and disposal is documented in the decommissioning summary reports.
5	Auditing	All assets will be erased of data using a certified Asset Disposal & Information Security Alliance (ADISA) or Security Equipment Approval Panel (SEAP) third party. This will produce an official erasure report for each asset to provide an audit of erasure after each erasure attempt. These will be collated and returned to Brunel University as evidence of the result of erasure attempts.

1.8 Glossary

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

ADISA	Asset Disposal & Information Security Alliance
BIL	Business Impact Level
CESG	Communications-Electronics Security Group
HMG	Her Majesties Government
IAS	Information Assurance Standard
IL	Impact Level (1-5)
RMADS	Risk Management Accreditation Document Set
SEAP	Security Equipment Approval Panel

SPF	Security Policy Framework
WEEE	Hazardous Waste Regulations, the Waste, Electrical and Electronic Equipment Directive

1.9 Legislation

The University will comply with all legislation and statutory requirements relevant to information and information systems, including:

- Computer Misuse Act 1990;
- Data Protection Act 1998;
- Communications Act 2003;
- Copyright, Designs and Patents Act 1988;
- Freedom of Information Act 2000;
- Human Rights Act 2000;
- Regulation of Investigatory Powers Act 2000;
- Police and Justice Act 2006;
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ('the Lawful Business Regulations');
- Employment Equality (Age) Regulations 2006;
- Employment Equality (Religion or Belief) Regulations 2003;
- Employment Equality (Sexual Orientation) Regulations 2003;
- Control of Substances Hazardous to Health (COSHH) Regulations 2002;
- Control of Lead at Work Practices 2002;
- Control of Asbestos Regulations 2006;
- Ionising Radiations Regulations 1999;
- Diseases and Dangerous Occurrences Regulations 1995;
- Social Security (Claims and Payments) Amendment (No. 3) Regulations 1993;
- Special Waste Regulations 1996;
- Construction (Design and Management) Regulations 1994;
- COUNCIL REGULATION (EC) No 1260/1999 laying down general provisions on the Structural Funds; National Minimum Wage Regulations 1999;
- Income Tax (Pay As You Earn) Regulations 2003;
- Lifting Operations and Lifting Equipment Regulations 1998;
- Provision and Use of Work Equipment Regulations 1998;
- Fire Precautions (Workplace) Regulations 1997;
- Employers' Liability (Compulsory Insurance) Regulations 1998

Additional guidance:

- Medical Research Council, Good Research Practice;
- Medical Research Council, Personal Information in Medical Research;
- Stated or implied requirements of UK Research Councils and other significant research sponsors. See Guidance on Managing Research Records which includes:

- ✓ Biotechnology and Biological Sciences Research Council (BBSRC)
- ✓ Economic and Social Research Council (ESRC)
- ✓ Engineering and Physical Sciences Research Council (EPSRC)
- ✓ Medical Research Council (MRC)
- ✓ Natural Environment Research Council (NERC)
- ✓ Particle Physics and Astronomy Research Council (PPARC)
- ✓ European Science Foundation
- ✓ The Wellcome Trust;

- HMRC Notice 700/21 Keeping VAT records;
- Information Commissioner's Office, Employment Practices Code (2005);
- Chartered Institution of Personnel and Development, Retention of personnel and other related records (2006);
- The National Archives, Records created by a public body fulfilling its obligations under the Freedom of Information Act 2000

1.10 Scope

University Confidential marked assets covered by this document include all magnetic and optical media, equipment containing magnetic media and printed documents, and any other asset used to process University Confidential marked data.

- Laptops (all models)
- Desktops (all models)
- Printers (all models)
- Servers
- Network equipment (routers, switches, firewalls)
- Optical Media (CD, DVD)
- External Storage Devices (USB Flash memory, Floppy Disk, Magnetic Tape Media, External Hard Drives)
- Particular requirements devices (X-Ray, Microfiche)
- Peripherals
- Paper

2. Policy

2.0 Computing Waste **MUST** never be disposed of through other General Waste routes. It is illegal to mix computing waster with General Waste or to landfill untreated computing waste**.**
University computers must also NEVER be sold to staff or any other individual organisations. If no use can be found within the University for unwanted equipment, or it is no longer functioning, it should be disposed of under the Agreement with the University's Authorised Contractor in accordance with this Policy. The final disposal route for all items must be recorded in the Asset Register.

If this policy is not applied, it will result in:

1) An infringement of relevant legislation including the Hazardous Waste Regulations 2005, the WEEE Directive 2007 and the Data Protection Act 2018; and
2) Where the infringement is deemed to be wilful, Brunel University disciplinary proceedings may be initiated.

The Brunel University approach towards disposal of assets is to remove data prior to removal from site. However, once the asset has been erased and contains no University Confidential data, there are several other considerations regarding the clean disposal or reuse that need to be addressed.

2.1 Disposal

This policy aims to ensure:

- Compliance with WEEE Directive (Waste Electrical and Electronic Equipment) through appropriate disposal of IT equipment.
- Compliance with the General Data Protection Regulation through secure disposal of personal data
- Deletion of confidential or sensitive non-personal data to avoid breach of confidence, breach of contract, commercial damage.
- Deletion of software which is under licence to avoid breach of licences.
- The University recovers any residual monetary value of IT equipment where appropriate.

It is University policy that:

- No IT equipment (including portable devices) may be disposed of other than by IS via the processes set out in the Secure IS Asset Disposal Process. Users with equipment which needs to be disposed of should contact IS to ensure the safe disposal of the equipment.
- All IT equipment must be disposed of in accordance with the University's Waste Management Policy.
- Prior to the disposal of computer equipment, all personal and sensitive data

must be securely destroyed by a method appropriate to the risk associated with the sensitivity of data and the equipment on which it is stored as set out in the Table A and Table B below.

- All other data and any software licensed to the University is removed prior to the equipment leaving the possession of the University.
- If IT equipment is disposed of by third party contractors on behalf of the University, they must adhere to the relevant standards and provide the relevant certificates of destruction and copies of waste consignment notes.
- University Confidential paper waste must be disposed of using the secure disposal bins provided.

The University operates a risk based approach which differentiates disposal techniques based on the user of the IT equipment and the type of data it is likely to contain, as outlined below:

Table A

Business Impact Level	Column B Release for re-use within the same or equivalent secure environment	Column C Release to any environment / Disposal	
		Non-destructive	Destructive
BIL1 (UNCLASSIFIED)	A	A	A
BIL2 (PROTECT)	A	B	A
BIL3 (UNIVERSITY CONFIDENTIAL)	B	C	B

Typically includes hard disk drives, floppy disks, USB removable hard drives (magnetic), zip disks and SCSI drives. Also includes software-encrypted disks. Commonly found in desktop or laptop computers, but can also be found in items such as servers or RAID arrays. Flash memory storage is used in mobile devices such as tablets and mobile phones and USB Flash drives.

Exceptions
Hardware encrypted disks including Full Disk Encryption (FDE) - see note in Additional Information; hard drives based upon flash or any other type of semiconductor memory, or hybrid drives. Procedures listed here must not be used for sanitising these devices.

Table B

Item	Data/Use	Risk	Proposed Method of data destruction	Reasons
PCs and Laptops	Standard office use on managed desktop and student PCs	Low	Overwriting drive multiple times	• Low risk of relevant data being on PC in the first place • Efficient in terms of volume of equipment, staff time, physical space
	Regularly used for processing personal data or sensitive personal data e.g. HR, Finance, Senior Managers	Medium	Overwriting drive multiple times	• Relevant data is likely to be present, therefore need for security outweighs operational efforts required • Will ensure data is effectively not recoverable • Data on laptops should be encrypted so if recovered will still be encrypted
	Used for processing non-personal confidential or commercially sensitive data	Medium	Overwriting drive multiple times	• Relevant data is likely to be present, therefore need for security outweighs operational efforts required • Will ensure data is effectively not recoverable • Data on laptops should be encrypted so if recovered will still be encrypted

	Research projects involving large amounts of sensitive personal data where data has been stored locally but not encrypted	High	Physically destroy	• Impact of data loss high, could lead to court action, severe reputational damage and loss of future research income
Servers	Storage of personal data, sensitive personal data and confidentiality of commercially sensitive data	High	Physically destroy	• Large volumes of data. • Mix of personal, sensitive personal, confidential, commercially sensitive data. • Disks are not in practice resold but are reused in other University systems until they fail or become obsolete
Other Portable devices	CDs, USB sticks (pen drives), floppy disks, memory cards, tapes	Medium	Physically destroy	• Simplest and most secure option. • With CD-Rs there is no option to overwrite • For CD-R should be undertaken as soon as the data is no longer needed to be stored in that way • For other removable media should be undertaken when the storage device is no longer needed.

	Larger USB drives, and external hard disks.	Medium	Overwriting drive multiple times	• Relevant data is likely to be present, therefore need for security outweighs operational efforts required • Will ensure data is effectively not recoverable

2.2 Multi-Function Devices, Photocopiers and Printers

Multi-function devices, photocopiers and printers have hard disks on which electronic copies of documents which have been photocopied, printed or scanned are stored during the operation of the device. Such hard disks must have their data removed by either data wiping or physical destruction which is dependent upon the level of risk associated with the device when it is decommissioned. As part of the contractual arrangements with suppliers, the University is provided with proof of data destruction when the device is returned on termination of the lease.

2.3 Smart Phones

All smart phones must have their data removed by being reset to factory default or by physical destruction dependent on the level of risk associated with the device and the data it has held when the device is decommissioned. If a device cannot be reset to factory default due to hardware malfunction then it must be physically destroyed.

2.4 Portable Media

Portable media which has, or had in the past, contained confidential and personal data should be disposed of in accordance with the above table.

2.5 Sale of IT Equipment

Where IT equipment has a residual value the University may choose to resell equipment if it is cost effective to do so. All sales will be undertaken in accordance with the University's waste disposal policy and the WEEE directives.

2.6 Records

- Consignment notes must be kept for a period of 3 years
- Waste transfer notes must be kept for a [period of 2 years

3.0 Asset Reuse

It is preferable to reuse the anonymised asset where possible as the greenest solution. It creates the least waste and uses less energy.

Where the asset can be reused, the redundant IT Asset is subject to testing, sorting, cleaning and refurbishment with some items at this stage failing to pass either functional or safety testing or criteria set for the successful redeployment or resale of the item. The failed items will be marked for disposal.

It is common practice for PCs to be moved between individuals and between Directorates and Faculties during their lifetime at the University. There are two risks associated with this practice:

- There is a risk that if a PC has been used for illegal purposes by one user, evidence of that activity will remain on the PC when it is transferred to a new user. This makes it unclear in any investigation as to who is responsible for any illegal activity.
- New users may have access to confidential or personal data which had been previously stored on the PC.

In order to mitigate this risk it is University policy that all PCs are data wiped when being permanently transferred from one individual to another following the three steps below:

The main steps in the decommissioning and cleaning of desktops and printers are:

- A site contact will be identified for each site by the BRUNEL UNIVERSITY LONDON prior to removal of the device to disposed of securely
- Brunel University's secure disposal supplier, will:
  - Wipe the disks to the required security standards.
  - Remove the desktops, servers and printers from site.
- Brunel University's secure disposal supplier will then dispose of the sanitised infrastructure and provide proof of disposal to Brunel University, who will produce a monthly decommissioning report.

Appendix A: Records Retention and Disposal Schedule

University Archives and Records Centre

Originating departments should retain all records which they need for their own operational purposes for as long as they need them. Records should only be transferred to the University Archive when they cease to be operationally relevant. Ref. University Archive Policy