Document Title:	**Information Asset Equipment Secure Disposal Policy**
Author(s) (name, job title and Division):	Lisa Megraw, DIG Project Manager, GOVRN
Version Number:	2.0
Document Status:	Approved
Date Approved:	17 October 2017
Approved By:	Data and Information Management Oversight Group (DIMOG)
Effective Date:	17 October 2017
Date of Next Review:	October 2018
Superseded Version:	1.0

Document History

Version	Date	Author/Consulted	Notes on Revisions
1.0	13 April 2016	DIG Steering Group	Approved by Steering Group.
2.0	09 Oct 2017	David Hannell, IT Services	1. Altered 5.2.3 to state 6mm for all items. 2. Update 6.3 from PMITS to UITGB. 3. Replacement of term “shall” with “must”.

Information Asset Equipment Secure Disposal Policy

1 Purpose

The purpose of this policy is to set out the principles to ensure that mechanisms are in place to protect University Information such that no electronic University Information remains discoverable on the equipment/ media/ device after it is disposed of by Cardiff University, that audit trails relating to the wiping and disposal processes are established and that responsibility for all actions is clearly and appropriately allocated. It is intended that this policy will work alongside the current WEEE guidance.

2 Scope

This policy covers all of the University's *Information Asset Equipment* and its disposal by members of the University.

3 Relationship with existing policies

This policy forms part of the Information Security Framework. It should be read in conjunction with the Information Security Policy and all supporting policies[1].

4 Policy Statement

The disposal of the University's *Information Asset Equipment* must be managed so as to ensure that information security risks are commensurate with the University's risk appetite and that internal and external information security requirements are met.

5 Policy

5.1 Recording of *Information Asset Equipment*

5.1.1 All items of *Information Asset Equipment* defined as requiring inclusion in an inventory (see section 8, below, for list of items) must be recorded on the section/ business unit inventory, together with the 'owner' where that equipment is portable and assigned to an individual, and any software licences associated with the equipment.

5.1.2 An audit trail must be retained that logs the wiping/ hard drive destruction process and wherever applicable connects it with the associated equipment on the section/ business unit inventory.

5.2 *Information Asset Equipment* containing *Classified Information*

5.2.1 Equipment for disposal must be wiped by an *IT Asset Disposal Service Provider* using software which meets or exceeds the Foundation Grade under the CESG CPA or CAPS scheme, or meets either the HMG Infosec Assurance Standard No. 5 enhanced or the DoD 5220.22-M for data sanitisation.

5.2.2 Where software cannot be used to wipe the data (e.g. backup tapes) another method of data destruction can be employed by an *IT Asset Disposal Service Provider* provided an independent data recovery specialist has verified that the method destroys all the device's data to the point that it is completely unrecoverable.

[1] http://sites.cardiff.ac.uk/isf/policies/

5.2.3 Where it is not feasible to wipe the equipment for disposal, it must be securely disposed of with the equipment shredded to at least 6mm particles for hard drives and digital memory as appropriate by an *IT Asset Disposal Service Provider.*

5.2.4 The equipment may not leave the University's secure premises for disposal or recycling unless the receiving *IT Asset Disposal Service Provider* is contracted with the University to provide a secure disposal process and accredited to the ADISA IT Asset Disposal standard[2].

5.2.5 Equipment to be reused internally must be reformatted and a fresh copy of the operating system installed onto the device before it is supplied to another school/ department or user.

5.3 *Information Asset Equipment* containing *Non-Classified Information*

5.3.1 Equipment must be disposed or internally reused in accordance with the guidance set out for each type of *Information Asset Equipment*.

5.3.2 Equipment for disposal must be wiped by an *IT Asset Disposal Service Provider*. The software used for wiping *Non-Confidential Information* is not required to meet CESG accreditation.

5.3.3 Where it is not feasible to wipe the equipment for disposal, it must be securely disposed of with the equipment shredded to at least 6mm particles for hard drives and digital memory as appropriate by an *IT Asset Disposal Service Provider*.

5.4 Contracting

5.4.1 All IT asset disposal or recycling services carried out by third parties must be carried out under contract with the contract specification including details of *Information Asset Equipment* wiping/ destruction, inventory and auditing requirements in line with this policy. Service providers must meet the specification and be signed up to the contract.

5.4.2 All *IT Asset Disposal Service Providers* under contract with the University must be audited to ensure that compliance with the contract specification in regard to information security is assessed annually.

5.4.3 Any staff member contracting a third party to carry out data processing using their own equipment must ensure that the third party has provided the necessary security assurances as set out in this policy in regard to the keeping and disposal of University data.

5.5 Secure Disposal Service

5.5.1 All *Information Asset Equipment* must be disposed of through a central service ran by Estates & Campus Facilities. Where exceptions are granted and signed off by a member of Estates with the delegated authority to do so as granted by the Director of Estates then the excepted party must be required to comply fully with the terms of this policy.

5.5.2 Parties granted exception from the central secure disposal service must be required to store any *Information Asset Equipment* for disposal in a designated, restricted access, locked location prior to collection by the *IT Asset Disposal Service Provider.*

[2] http://www.adisa.org.uk/members-list/

5.5.3 Parties granted exception from the central secure disposal service will be required to follow the same audit trail process as the central service, including where applicable, the use of barcodes.

5.6 Review

5.6.1 This policy and associated guidance should be reviewed annually to ensure that it covers any emerging technologies and is in-line with the University's risk appetite.

6 Responsibilities

6.1 The Director of Estates & Campus Facilities is responsible for ensuring that appropriate processes and procedures are established and maintained to support this policy. The Director is also responsible for ensuring that all external *IT Asset Disposal Service Providers* used in connection with this policy meet the applicable specifications and contracting terms outlined above.

6.2 Heads of section/unit are responsible for ensuring that *Information Asset Equipment* is recorded in the Inventory wherever applicable and that any barcodes required in order to establish an audit trail are added to the equipment in accordance with this policy by their section/unit. They are also responsible for ensuring that any equipment for internal reuse is wiped in accordance with this policy before it is handed over to another school, department or user.

6.3 The Director of University IT (UITGB) is responsible for reviewing the technical standards set out in this policy to ensure they remain appropriate and in line with ICO recommendations.

6.3 It is the responsibility of all University Members to ensure that they uphold the principles set out in this policy and comply with any appropriate processes and procedures related to this policy.

7 Compliance

Breaches of this policy may be treated as a disciplinary matter dealt with under the University's staff disciplinary polices or the Student Disciplinary Code as appropriate. Where third parties are involved breach of this policy may also constitute breach of contract.

8 Definitions

Information Asset Equipment: Covers the following University owned items of equipment: computers, servers, laptops, tablets, mobile phones, solid state drives, external hard drives, server/computer backups on tape or disk, USB sticks, CDs/DVDs and other storage media, printers, scanners, audio/ visual recording equipment and storage systems (e.g. storage arrays).

Information Asset Equipment for Inclusion in Inventory: All University owned computers, servers, laptops, tablets, mobile phones, server/computer backups on tape or disk, solid state drives, external hard drives, printers and scanners.

Classified Information*:* Information that is confidential, highly confidential or requires enhanced protection to ensure integrity or availability due to its nature. A detailed breakdown of the University's confidentiality classification system can be found in the University's Information Classification document[3].

University Members*:* University Members are as defined in Statute and Ordinances.

IT Asset Disposal Service Provider: A third party who is contracted to carry out IT Asset disposal or recycling services on University owned equipment.

Third Party Contractors: Any party who is not defined as a University Member who has an agreement with the University to supply a service.

[3] http://sites.cardiff.ac.uk/isf/handling/