University of Liverpool

IT Asset Disposal Policy

Reference Number	CSD-015
Title	IT Asset Disposal Policy
Version Number	v1.2
Document Status	Active
Document Classification	Open
Effective Date	22 May 2014
Review Date	28 March 2018
Author	Computing Services Department (David Hill)
Approved by	Corporate Services & Facilities Committee (Jan 2014)
Implemented by	Information Security Officer
Monitoring of compliance	Faculty Information Security Managers
Comments	• **22/05/2014 - Annual Review/Update v1.0 – v1.1** • **31/07/2015 – Annual Review/Update v1.1 – v1.2** • **29/07/2016 – Annual Review** • **28/03/2017 – Annual Review**

Contents

1. Introduction

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 IT equipment we use. The IT Asset Disposal Policy and its associated policies are concerned with managing the secure disposal of IT equipment assets which are owned by the University and are no longer required.

2. Principles

This policy defines the roles and responsibilities of staff in ensuring the secure disposal of University IT equipment.

- All staff/student(s) of the University who use information assets have a responsibility to handle them appropriately and in accordance with their classification
- 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. Information assets that are used in conjunction with the IT asset must also be accurate, complete, timely and consistent with other related information and events.

3. Objectives of This Policy

- To define the responsibilities of individuals for the secure disposal of University IT assets
- To provide a rigorous and consistent process to ensure University IT 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, mobile phones and other devices that process and store University data.
- To provide advice on the appropriate methods of destruction of physical media.
- To ensure sensitive information assets stored via the 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.

4. Action Implementation

Procedures will be put in place to ensure effective use of the University IT Asset Disposal Policy. These procedures include:

- Clear identification of University information assets and protection in line with the asset classification scheme.
- Implementation of procedures for the disposal of University IT assets.
- Ensuring that disposal procedures are adhered to.
- Provision of certification and audit trail for asset disposal.

5. Background

University information assets which are sensitive or valuable must be protected at all times. Consideration must be given to how the assets are handled during day-to-day activities; how they are protected outside normal working hours; and how they are protected when accessed either on or off campus. It is also crucial that this consideration is extended to the disposal of equipment on which sensitive or valuable data has been accessed, processed or stored.

All information must be classified by those who own or are responsible for them. For more information, refer to the Information Asset Classification Policy.

6. University Disposal/Destruction of Physical Media

The University has a number of cross cut shredders and confidential waste consoles across the estate which must be used to dispose of hardcopy sensitive information assets which are no longer needed. This removes the need for staff/student(s) of the University to store unwanted information assets within their workspace areas and improves efficiency.

For all other asset types such as, but not limited to:

- CDs
- Floppy discs
- Video tapes
- X-Rays
- Microfiche records
- Paper-based and hardcopy documents

Please refer to Records Management in the first instance

Tel: 0151 794 5675 (Internal) or Email: recman@liv.ac.uk for more information.

7. Identification of IT Equipment Assets

IT equipment and devices that have the ability and capability to store University information and sensitive data include:

- PCs
- Laptops
- Mobile phones
- Multi-Functional Devices - printers/scanners
- Servers
- USB memory sticks and external hard drives

Asset Tags

Staff/student(s) should be aware of the origin of the IT equipment being used to fulfil University business activities. All IT equipment which has been purchased via a University account must have an asset tag assigned to it. Where practical, the asset tag will be physically visible on the equipment stipulating that it is the property of the University of Liverpool.

In the event that you are unsure of the origins, responsibility and ownership of IT systems or equipment, contact the CSD Service Desk.

8. Scope of Destruction

Staff/student(s) of the University must follow the approved destruction methods to ensure unauthorised exposure to University's information assets is minimised. Equipment that stores sensitive data, which is no longer needed or has reached "end of life", **must** be securely deleted and sensitive data deemed unreadable and unrecoverable **before**:

- Re- distribution or re-use within the University
- The equipment leaves University premises
- Decommissioning of core services

Such equipment must be securely wiped or removed by CSD or an authorised delegate only and in accordance with the University disposal criteria (see section 9). CSD will undertake or manage the work to ensure the risk of unauthorised access to sensitive data is minimised.

9. University Disposal Criteria

In the event that sensitive information and IT assets are no longer needed for University purposes and cannot be securely wiped the equipment may need to be physically destroyed.

Removal / Reformatting of Storage Disks

IT equipment disposal must be managed by CSD and approved delegates only. Deleting visible files is not a sufficiently secure method of wiping equipment - data recovery software could be used by a new owner to "undelete" such files.

Similarly, formatting the whole hard disk or storage device may not prevent the recovery of redundant data as it is possible for disks to be "unformatted".

Software/Sanitisation/Destruction

Any IT assets leaving University premises must comply with licences and copyright law. CSD must ensure that all University licensed software or operating systems are removed.

Any sanitisation or wiping undertaken by or on behalf of the University must meet the following minimum standards:

- **HMG Information Assurance Standard No: 5**
- **U.S Department of Defence 5220.22m**
- **Common Criteria EAL 3+ certification**

CSD IT Asset Disposal Scheme

IMPORTANT – All University owned assets must be disposed of using the CSD disposal service. University assets must not leave University premises without CSD's permission or knowledge.

Reuse and redistribution of IT Equipment

CSD will undertake the necessary secure procedures to ensure any sensitive data is removed before IT equipment is redistributed.

Certification and Audit

Successful deletion and destruction must be evidenced and certification must be obtained and recorded at all times.

Asset Inventory

Details must be recorded and updated within the CSD Inventory database to ensure the University has an up-to-date record of active IT assets.

IT Disposal Services

<table>
<tr><th colspan="3">CSD Disposal Services</th></tr>
<tr><th rowspan="2">PC Scheme
(*End of Warranty Disposal)</th><th colspan="2">Individual Requests</th></tr>
<tr><th>Single Device(s)/On Campus</th><th>Multiple No of Devices/Heavy Load items/Remote Campus</th></tr>
<tr><td rowspan="3">The scheduled service should be considered as the main channel for pickup/disposal throughout the University.

CSD will pick up and remove the existing device via the PC Scheme and replace it with a new PC once the warranty of the existing PC has expired.

For more information on the PC Scheme and the warranties of IT assets please refer to CSD PC Scheme web pages in the first instance.</td><td rowspan="3">IT Assets will be removed/disposed of within an agreed timeframe with CSD and the requestor.

Typical Individual requests consist of:

• Single PC/laptop devices that are no longer required for day to day use
• Single PC/laptop devices that can be recycled/re-used throughout the University
• Single PC/laptop devices that are required to be securely deleted prior to re-use e.g. new starter or for regulatory purposes</td><td>Significant numbers and bulk IT assets (in the same location) may be required to be removed due to:
• Repurpose of building/room
• IT/Network upgrade and redundant kit
• Completion of academic/professional contracted Works</td></tr>
<tr><td>Heavy Load Items consist of:
• Multiple Servers
• Multiple PC Base Units
• Multiple Monitors
• MFD Printer</td></tr>
<tr><td>Remote Campus consists of any UoL location outside of City Centre Campus.</td></tr>
<tr><th colspan="2">There are no additional charges for these services</th><th>There may be additional charges for these services</th></tr>
<tr><td colspan="3">Urgent (immediate disposal)</td></tr>
<tr><td colspan="3">IT devices that have been used for sensitive work and/or cannot be protected from external threats or miscellaneous tampering on a day to day basis.</td></tr>
<tr><td colspan="3">Non-Urgent (scheduled disposal)</td></tr>
<tr><td colspan="3">IT devices that have NOT been used for sensitive work and CAN be protected from external threats or miscellaneous tampering on a day to day basis.</td></tr>
<tr><td colspan="3">CSD Physical Review</td></tr>
<tr><td colspan="3">Upon receiving the initial urgent disposal request, CSD will arrange with the requestor to physically review the IT assets prior to collection/disposal.</td></tr>
<tr><td colspan="3">All individual requests must be made by completing the IT Disposal Request Form.</td></tr>
</table>

10. Data Backup

It is the explicit responsibility of the owner/requestor of the IT asset to ensure that all relevant data has been sufficiently removed from the IT device and backed up **before requesting disposal and/or prior to the scheduled pickup**.

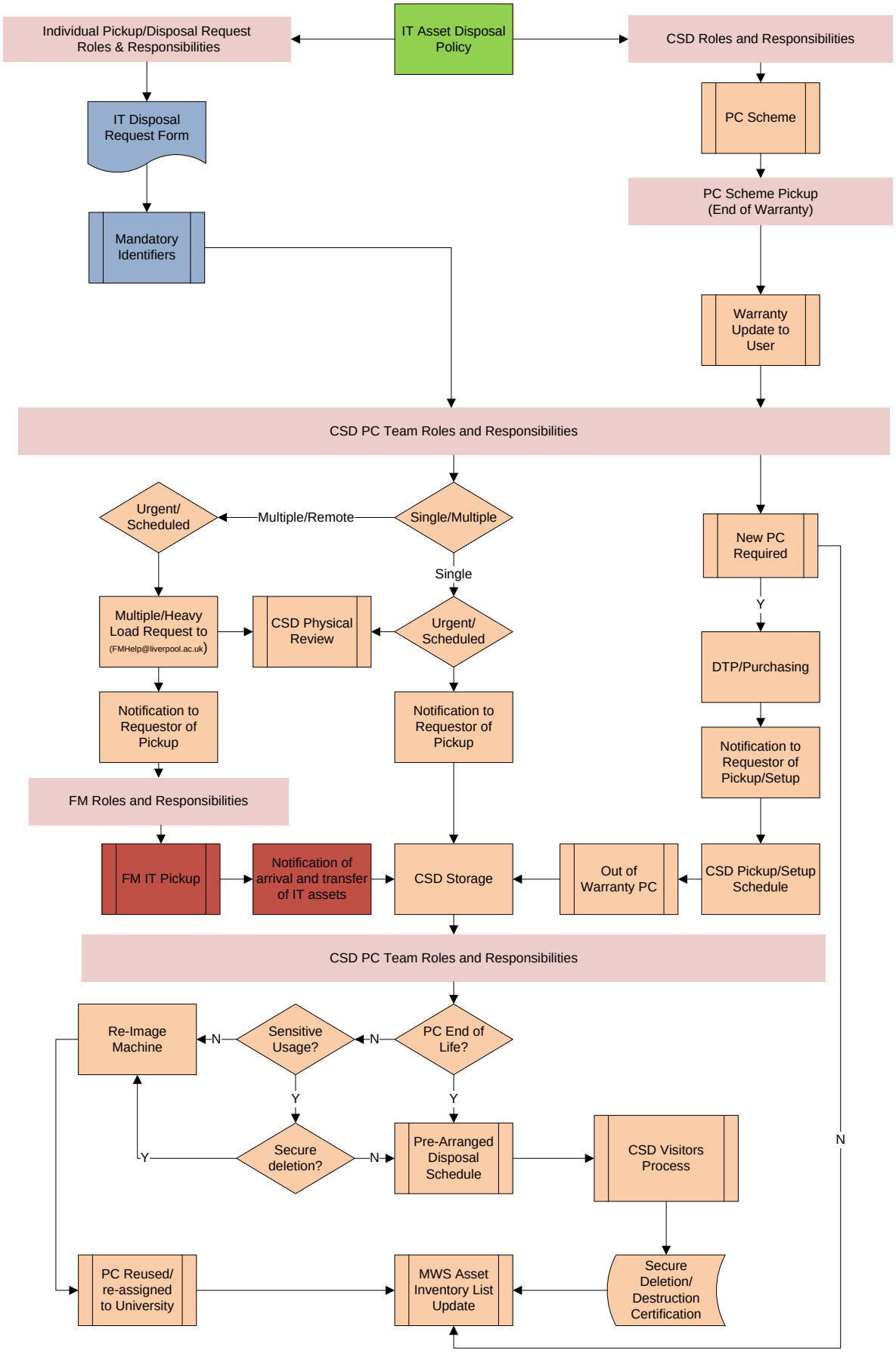
Once the system is in CSD's possession, all data will be securely sanitised and made unrecoverable. CSD will not be responsible for saving or removing any residual data.

11. Physical Security

IMPORTANT – This is not a storage service. It is the responsibility of the owner/requestor of the IT equipment to ensure the device is physically secure during its use and prior to collection for disposal.

For more information on securing IT equipment and devices please refer to the Workspace and IT Equipment Security Policy.

12. IT Asset Disposal Process



IT Asset Roles and Responsibilities

Requestor

All IT disposal requests must be requested via an IT Disposal Request Form is completed and submitted to CSD.

All mandatory fields must be completed prior to submission. Failure to supply the relevant information may defer or delay collection/disposal. CSD will only carry out the secure disposal of the IT assets detailed within the initial request. Any additional IT assets will require a separate request.

CSD/Information Security/Approved Third Party

Once the disposal request has been received, CSD will schedule a collection with the requestor.

CSD will ensure:

- All **Urgent disposal requests** will be physically reviewed, picked up and stored within CSD storage and disposed of in a secure manner within an agreed timescale
- All Scheduled disposal requests will be picked up and disposed of in a secure manner within an agreed timescale
- Certification of secure disposal will be obtained
- The redistribution or disposal of IT assets will be recorded in the asset inventory database

Facilities Management (Multiple No of Devices/Heavy Load/Remote Campus)

In the event of a significant disposal request, CSD may request that Facilities Management collect and transfer the IT assets to the appointed CSD storage.

13. Approved Third Party Supplier/Service Provider (Licensed)

Where a licensed third party service provider is to undertake secure disposal/destruction on behalf of the University, CSD will ensure the University disposal criteria can be satisfied and all confidential or sensitive information is securely sanitised and safeguarded.

It is imperative that a formal contract, due diligence and security review of the third party supplier is undertaken at least on an annual basis to ensure University requirements are satisfied. Please refer to the IT Procurement and Third Party Security Policy and Information Security Review Policy for more information.

14. Decommissioning and Core Network Infrastructure Changes

Non-authorised members of staff must ensure that any request to recycle, remove, decommission or change an IT asset from the core network or infrastructure is **undertaken by or on advice from CSD**. This ensures that any changes, impacts and risks to the confidentiality, integrity and availability of information and IT assets are fully considered by an appropriate staff member of the Computing Services department.

15. CSD Service Desk Contact Details and Service Times

For all other CSD services and queries please refer to the CSD Service Desk in the first instance. You can do this by:

- Logging an online support request: http://servicedesk.liverpool.ac.uk/
- Email: servicedesk@liverpool.ac.uk
- Telephone: 44567 (internal)
- Telephone: +44 (0) 151 794 4567 (external)

16. Legal obligations and University policies

This policy is aimed at all members of the University who have a responsibility for the use, management and ownership of information assets. This policy is part of the University Information Security Management System (ISMS) and should be read in conjunction with the **Information Security Policy** and its sub policies and relevant UK legislation. Further relevant policies and legislation are listed in **Appendix A**.

17. Compliance and Monitoring

All members of the University are directly responsible and liable for the information they handle. Members of staff are bound to abide by the University IT regulations by the terms of their employment. Students are bound to abide by the University IT Regulations when registering as a student member of the University.

Authorised members of the University may monitor the use and management of information assets to ensure effective use and to detect unauthorised use of information assets.

Appendix A – University ISMS Reference

- Regulations for the Use of IT Facilities at the University of Liverpool
- JANET Acceptable Use policy
- Information Security Policy
- Workspace and IT Equipment Security Policy
- Information Security Incident Response Policy
- Information Asset Classification Policy
- Information Security Review Policy
- IT Procurement and Third Party Security Policy
- Security Investigation Policy
- Procurement Policy
- Social Media Compliance Policy
- Data Protection Policy
- Freedom of Information Policy
- Copyright Policy
- Card Payment Policy
- Records Management Policy
- Records Retention Policy
- Risk Management Policy
- Student/HR Disciplinary Procedures

Relevant legislation includes:

- Data Protection Act 1998.
- Human Rights Act 1998.
- Regulation of Investigatory Powers Act 2000.
- Freedom of Information Act 2000.
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
- Computer Misuse Act 1990.
- Copyright, Design and Patents Act 1988.
- Copyright (Computer Programs) Regulations 1992.
- The Terrorism Act 2000
- The Anti-Terrorism, Crime and Security Act 2001.
- Official Secrets Acts 1911-1989.
- Obscene Publications Act 1994.

Relevant Regulation includes:

- PCI-DSS (Payment Card Industry Data Security Standards)