Document Reference Number	**UoG/ILS/IS 019**
Title	Policy for IT Asset Management & Disposal
Owning Department	Information and Library Services
Version	1.0
Approved Date	30/08/2023
Approving Body	IT Management Board (IM)
Review Date	09/07/2024
Classification	Public – Non-Sensitive

UNIVERSITY of GREENWICH

Policy for IT Asset Management & Disposal

1.0 Purpose

1.1 To ensure all University of Greenwich IT Assets are correctly managed and disposed of throughout their lifetime with the University. This includes:

- Compliance with the University's Information Security, Data Protection, Information Compliance & Sustainability Policy.
- 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.
- Compliance with WEEE Directive (Waste Electrical and Electronic Equipment) through appropriate disposal of IT equipment.

2.0 Scope

2.1 This policy governs corporately managed IT assets owned by the University of Greenwich. University-owned IT assets include but are not limited to desktops, laptops, tablets, hard drives, USB and portable storage equipment, smartphones, audio visual equipment, cameras, desktop printers, monitors and docks. The following items are out of scope of this policy: MFDs, servers, networks switches, wireless access points, specialist lab equipment (such as microscopes or raspberry pi's), tills, BMS and CCTV equipment. IT Assets purchased by the University but owned by third parties are also out of scope.

2.2 The policy applies to all University staff, contractors, and third-party agents.

3.0 Reference to International Organisation for Standardisation (ISO) 27001

3.1 This policy complies with the University's Information Security Strategy and draws upon the ISO 27002 Code of Practice.

4.0 Principles:

4.1 IT Assets are defined as any items within scope purchased with University money or funds granted directly to the University or schools for research and education purposes.

4.2 University hardware assets should always be branded with a "UG" asset tag with unique UG number applied to the outer casing of the device on purchase. Any

hardware that cannot be tagged due to its size or shape will remain property of the University and will be subject to the same policies. Asset tags must not be deliberately removed or defaced. Staff are individually responsible for returning their device to the IT Service Desk to be retagged if the asset tag begins to deteriorate. Staff without a UG asset tag on their device should contact the IT Service Desk for advice.

4.3 A standard IT provision will be issued to all new starters. All standard devices will be managed and fully supported. Non-standard IT Assets will require business justification and any agreed non-standard devices may only be supported on a 'best effort' basis; this will be agreed at the time of purchase and/or approval.

4.4 All IT assets will be purchased following procurement purchasing rules and utilise existing frameworks whenever possible.

4.5 IT Assets shall remain property of the University and must be returned to the appropriate line manager or the IT Service Desk when leaving the University or when the device is no longer required for work. The device cannot be retained.

4.6 Where a device is purchased as part of an externally funded project and the project is transferred to an alternative institution, approval must be sought from the Faculty Operating Officer for the device to be transferred along with the funding. Approval will be subject to the terms of the research funding.

5.0 Responsibilities of those who manage IT Assets

5.1 Detailed records of University IT assets (excluding consumable items e.g. keyboards, mice etc.) are maintained by Information and Library Services (ILS) in a central asset inventory. Each record includes but is not limited to the make, model, serial number, UG number, device owner, owner's department, purchase order, device location, warranty end date, purchase date and device status. IT assets not allocated to named individuals, such as shared desktop PCs & laptops, will be allocated to a school or department rather than an individual person.

5.2 The IT Asset inventory must be updated in the following instances: a newly purchased device is received or allocated, an existing device is transferred to another member of staff, disposed of, lost, or stolen and when any fixed IT asset location changes.

5.3 IT Assets returned to IT Service Desk for any reason must be wiped and reallocated if still within the device's five-year life span.

5.4 All IT Assets will be disposed of by ILS and will follow the University's IT Asset Disposal policy.

6.0 Responsibilities of all IT Asset Users

6.1 IT Assets must not be used by any third-party including friends and family.

6.2 Loss, damage or theft of an IT Asset must be reported immediately to the IT Service Desk.

6.3 Assigned owners of devices, or departments/schools for shared devices, will always be responsible for the care and security of IT Assets whether in use, storage or movement. The device owner's faculty or department may be held financially responsible where there is physical or financial loss due to theft, mishandling or accidental damage.

6.4 All repairs of IT assets must be coordinated via the IT Service Desk. Repairs should not be undertaken personally or through any other third party as this may invalidate the warranty and/or associated support agreements. Costs incurred from unauthorised repairs will not be reimbursed.

6.5 Users shall not install unapproved software on devices. Requests should be made to the IT Service Desk via the AMP process to have additional software that is not already on the device or available to install from Software Center. Any software installed must be legitimately purchased and appropriately licensed for its intended use.

6.6 Upon terminating employment with the University, staff must return all devices assigned to them. A list of assigned devices will be produced and issued to the staff member and their line manager to help ensure all devices are returned before their last day. Line managers will be responsible for ensuring all IT Assets are returned when the staff member leaves. Any device not returned 10 days after the final day of employment will be deemed as lost\stolen and the lost\stolen asset process will be followed by the IT Service Desk.

6.7 It is recommended that laptops are taken home every night to ensure that staff can continue their work in the event of the University needing to close at short notice. If for any reason a laptop is left on-site overnight, it must be securely locked away. To minimise the risk of theft, laptops should not be left unsupervised in unsecured areas while on-site.

6.8 Where a member of staff is transferring departments or schools within the University, they are permitted to take their laptops with them but must inform the IT Service Desk prior to moving.

6.9 IT Assets should not be transferred between individuals and must always be returned to the IT Service Desk for reallocation.

7.0 IT Asset Disposal

7.1 To ensure that appropriate arrangements for secure data erasure and IT equipment disposal are in place and comply with:

- WEEE directive (Waste Electrical and Electronic Equipment) and the University's policies and guidelines.
- Data Protection legislation relating to the secure disposal of personal data in digital form (Refer to the Information Compliance Code of Practice 6 – Retention and Disposal of Records and Data).
- License conditions for specific software.

7.2 All University IT equipment is to be disposed of by an approved University service provider, managed by ILS. The contract with the provider will ensure that the service is compliant with the WEEE directive and that data on the equipment is removed. Proof of equipment disposal and (if applicable) data erasure or destruction must be provided by the disposal company.

7.3 IT equipment shall not be disposed of by any means other than the processes set out in this policy**.** Users with equipment which needs to be disposed of should contact the IT Service Desk to ensure the safe and secure disposal of the equipment. ILS staff will then ensure the equipment is reused or disposed of as appropriate, including the deletion of any data in accordance with this policy.

7.4 All IT equipment awaiting disposal will be kept in a secure storage area until collection by the contracted service provider.

7.5 After the contracted service provider has collected the Item or the item has been repurposed, the IT Asset record must be updated to reflect the change in status. Copies of the erasure and disposal certificates issued by the contracted service provider will be recorded and linked to the individual asset items to end the IT asset lifecycle process.

7.6 Sale or gift of University IT equipment to individuals, for example, when they leave employment is **strictly prohibited**; equipment cannot be passed on to third parties and no IT equipment should be offered to others via the University's Yammer.

7.7 Where possible, and in support of the University's Sustainability Strategy and Policy which promote a 'zero waste' principle, reusing unwanted University IT equipment is promoted. For internally reused IT equipment, the IT Service Desk should be consulted first, to ensure any data is wiped prior to reuse. For external reuse, an approved University service contracted by ILS must be used to comply with the WEEE directive.

8.0 Policy Compliance

8.1 The necessary steps to verify compliance to this policy shall be undertaken. This includes, but is not limited to, business tool reports, internal and external audits and feedback to the policy owner.

8.2 Failure to adhere to this policy will be addressed under the University's disciplinary processes and relevant contractor and third-party contractual clauses relating to non-conformance with the Information Security policies.

9.0 Exception to Policy

9.1 Any exception to this policy must be approved by the Executive Director and CIO or a nominee.

10.0 Policy Review and Maintenance

10.1 This policy shall be reviewed annually and where necessary will be updated as part of the continual improvement process.

11.0 Related Policies Links

Links to Information Security Policies,
Links to the Information Compliance Policies,
Links to Sustainability Policy
Links to Software Policy