UNIVERSITY OF WESTMINSTER

IT Asset Management Policy

Policy Title	**IT Asset Management Policy**
Policy Date	**23rd November 2022**
Approving Body	**University Secretary and Chief Operating Officer**
Version	**2.3**
Supersedes	**IT Asset Management Policy 2.2**
Publishing	**Public, University website**
Related Policies and documents	**Internal policies on University SharePoint** • **Information Security Policy** • **IT Acceptable Use Policy** • **Sustainable Procurement Policy** • **IT Administrator Policy** • **Patching Policy** • **IT Decommissioning and Disposal Policy**
Policy Owners	**Russell Poole, Director of Information Systems and Support**
Lead Contacts	**Ian Dickens - Head of IT Operations, ISS** **Richard Willett - Asset Management Lead, ISS**

Revision History

Version	Summary of changes	Date	Author(s)
1.0	First Publishing	17/01/2020	
2.0	Full review and updated of 2020 policy	18/3/2022	R. Willett
2.1	Draft review completed: 14 sections updated	14/4/2022	R. Willett I. Dickens N. Buckley
2.2	Extended review from Senior Management and ISS Team & Tech Leads: 59 updates accepted 4 rejected	03/5/2022	R. Willett
2.3	Minor updates to 13 sections	13/9/2022	R.Willett

1. Introduction

1.1. This IT Asset Management Policy provides a framework for the appropriate and effective management of IT equipment (hardware and software) throughout the lifecycle of that asset.

1.2. It defines responsibilities that relate to the implementation of this policy and is designed to ensure that IT assets are:

- Managed appropriately from their procurement to disposal in a way that is compliant with the University's policies and regulatory obligations;
- Procured correctly in line with the UK procurement regulations and University purchasing processes included in the University Sustainable Procurement Policy;
- Registered within Information Systems and Support's (ISS) asset management system for tracking and auditing purposes;
- Supported and maintained throughout their lifecycle so that they remain compliant, and deliver value for money;
- Controlled effectively to protect the data and information that they store or transmit; and
- Administered for the identification of risk and business continuity planning.

2. Scope

2.1. This policy applies to all IT assets purchased by or on behalf of the University of Westminster, including those purchased for the University of Westminster Student's Union (UWSU), the Regent Street Cinema, and any other affiliated companies for which the University purchases or provides IT assets, including those which may be fully or partially funded by research grants, or acquired to provide accessibility to work.

2.2. An IT asset is defined as:

- All desktop and laptop computers;
- All monitors, printers, scanners, and portable storage devices;
- All mobile phones, smartphones, tablets, and other portable computing equipment;
- All IT and audio-visual (AV) equipment;
- System software, client applications and associated licences;
- Any other IT peripheral costing £100 or more.

2.3. This policy also applies to all IT assets that form part of the University's IT infrastructure (servers, routers, firewalls, switches, access points and other network infrastructure etc., including both physical and virtual devices and Cloud services) and any equipment that electronically stores data on the University's central file storage systems or transmits it across the network.

2.4. This policy applies to all students, colleagues, and other associates of the University, including agency staff, contractors, partner organisations, suppliers, and customers, who request or hold IT equipment purchased by or on behalf of the institution.

2.5. Specialist IT equipment used in the support of curriculum delivery, not covered in the description in clause 2.2 or 2.3 (such as laser cutters, blood pressure monitors, mixing desks etc.) is not included in the scope of this policy. This specialist equipment is procured and managed by each College in accordance with their asset control policies and procedures but must also comply with the IT - Acceptable Use Policy if there is a capability to locally store data or connect to the University IT network.

2.6. Information asset management is covered in the Information Security Policy

3. Management of IT Assets

3.1. All IT assets purchased by the University are the property of the University and will be managed, deployed, and used by ISS on behalf of the University in a way that is deemed most effective for addressing the University's needs to deliver learning and support services, in a way that provides best value for money.

3.2. Endpoint devices; including laptops, desktops and mobile phones will be provided with a 5-year lifespan and replaced at the end of this period unless required to be replaced earlier through failure or loss.

3.3. The budget for IT assets will be centralised and managed by ISS on behalf of the University with the exception of research grant awards as in section 3.11, College budgets used to purchase specialist IT equipment described in clause 2.5, and DSE (Display Screen Equipment) equipment as per 3.13. Additional exceptions which may require funding contributions to be made following consultation with ISS will be managed on a case-by-case basis.

3.4. All requests for IT assets must be submitted to ISS via the IT Service Desk portal.

3.5. IT assets will be issued in line with the relevant standard for the user's role in accordance with the approved hardware and software list published in SharePoint and will be recorded as assigned to the user for the duration that they are carrying out that role, after which time the asset should be returned before redeployment to the next user in that role. IT assets are allocated to support the requirements of specific roles and are not to be redeployed to other individuals, teams, departments, or schools even if the role is similar to another.

3.6. The University will issue laptops (and associated peripherals) only to colleagues; desktop machines will only be deployed to learning spaces and shared usage spaces e.g. at library or Registry counters. Any other use cases will be handled on a case-by-case basis following the submission of a business requirement and detailed use case via the Service Desk, or the presentation of a completed DSE or accessibility assessment. Any computer systems which are provided will remain under the management of ISS and subject to the terms of this policy and IT Acceptable Use Policy.

3.7. Students and colleagues may be granted permission to make use of loan laptops following a request using the loan laptop process. These laptops will remain under the management of ISS and are only permitted to be used under the terms of the loan agreement. Loaned devices must be returned to ISS once they are no longer required, or in the event that ISS requests their return along with all peripherals that were allocated with them. At the end of the loan period all equipment must be returned to ISS including any peripherals that were also provided.

3.8. The University will issue individual devices to all colleagues in substantive roles. It is assumed that colleagues employed on a 'student helper', part time visiting lecturer (PTVL) or similar type contract will be only accessing shared usage spaces and as such may not be provisioned with an individual device. In the event that individual devices are required by PTVLs, a request can be submitted for one to be provided but these will be assessed by ISS on a case-by-case basis.

3.9. ISS will assess requests for new and replacement IT equipment and fulfil them with standard IT equipment that best fit the requirement by aiming to reissue existing assets in the first instance. Where a member of staff changes role within the University the device must be made available for redeployment to the incoming staff taking over that role and be returned to ISS to ensure this is ready the next user of it. ISS will not purchase new devices for incoming staff unless:

a. A device being used by that role is within 6 months of the end of warranty.
b. The incoming user is taking on a newly created role at the University.

3.10. Any IT asset returned to ISS will be assessed for continued suitability before being reissued. This may result in a different make/model being issued than was returned but will remain a suitable specification for the role. In the event that an asset needs to be returned but cannot be immediately replaced every effort will be made to provide a suitable loan device on a temporary basis, however this may not be of equal specification to the original device.

3.11. Requests for non-standard IT equipment or specialist IT equipment should also be made on the appropriate form on the IT Service Desk portal and will be assessed within ISS. If approved, ISS will cover the full cost of the equipment as per 3.2 in most circumstances with any exceptions managed on a case-by-case basis. Any non-standard IT equipment issued will be subject of this policy and IT Acceptable Use Policy if it meets criteria in sections 2.2 or 2.3 and may be subjected to a risk assessment carried out by ISS which may result in the equipment being subject to specific terms of use or configuration restrictions stipulated during the request approval.

3.12. Only one IT asset of each type will be issued per person; the only exception to this request is where a colleague may need an additional device for research purposes or to assist with an accessibility requirement. These requests will be assessed on a case-by-case basis; all costs for additional devices will need to be wholly covered by the requesting department or evidenced by a supporting research grant award as part of the request. Any additional IT equipment provided in this manner will remain under the management of ISS and subject to the terms of this policy and the IT Acceptable Use Policy.

3.13. For non-standard and specialist IT equipment, including those for PhD students and research purposes, only those which following consultation with ISS and that meet the minimum standards as detailed in the hardware standards on SharePoint will be approved for purchase and subsequent connection to University systems, this includes those purchased for research purposes. Any IT asset deployed in this situation will remain the property of the University under the management of ISS and subject to the terms of this policy.

3.14. The cost of IT related reasonable adjustments for colleagues with disabilities will be met by the requesting department. This includes software and equipment recommendations following approved DSE assessment, however any purchases which alter the way that IT equipment is used should be carried out in consultation with ISS as per 3.15 prior to any purchases being made.

3.15. ISS will not, without adequate and suitable further justification, approve or proceed with the procurement of IT assets that do not comply with the requirements of the University's plans, policies and standards.

3.16. The procurement of IT assets must be undertaken in consultation with and carried out by ISS, including where the asset is being wholly purchased by funds from another department or research grant in order to ensure the asset is compliant with the relevant standards and can be recorded as such. Any IT assets purchased without consultation with ISS will not be permitted to be used on the University network, have any ISS managed licensed software installed, or be eligible for any ISS support. Any non-ISS managed IT equipment that is connected to the University network will be treated as a breach of this policy and subject to disciplinary proceedings.

3.17. ISS is responsible for engaging with the University's Procurement Team and ensuring that the procurement of IT assets is in line with published best practice and University financial regulations.

3.18. On behalf of the University and in consultation with the Procurement Team, ISS is responsible for identifying and managing sources and channels for the purchase of IT assets, utilising existing framework agreements whenever possible.

3.19. All approved devices and applications will be recorded in the University's published hardware and software lists once they have been assessed, tested, and procured following the agreed procedures.

3.20. All IT assets defined in 2.2 will be registered in the ISS Asset Management System and be asset tagged before being issued or put into use. Once in use, information about assets will be maintained by ISS in the Asset Management System, to enable them to be tracked, managed, and audited throughout their life cycle.

3.21. All IT assets purchased by the University will be stored in University controlled asset management stores managed by ISS, or by a third-party company contracted to do so, when they have not been issued or are not in use.

3.22. IT assets will be adequately administered and maintained to ensure they remain fit for purpose and compliant with the licenced conditions of use during their entire lifecycle. The University retains the right to collect and/or inspect the equipment at any time, and to alter, add or delete installed software or hardware in order to remain compliant. All users of IT assets agree to support this process and comply with all required audit or maintenance instructions including regularly connecting devices to the University network to allow updates and security patches to be applied in accordance with the patching policy. Any computer that has not been connected to the network for more than 3 months will be disabled.

3.23. All IT assets must be assigned to an individual user (or for shared machines e.g. at library or Registry counters, a named individual within a department), who will be held responsible for their care and security at all times whether they are in use, storage or being transported and will need to ensure they are protected against physical or financial loss whether by theft, mishandling or accidental damage by using appropriate physical security measures.

3.24. Where an IT asset is lost, stolen or damaged, this should be reported immediately to the IT Service Desk, and in addition to the police where relevant. IT assets that are lost or stolen will be sent a command to be locked and wiped. These assets will be marked with the status of lost or stolen in the asset management and a register of incidents will be kept by the IT Service Desk for monthly security reporting and any other appropriate reporting requirements.

3.25. ISS will replace devices that have been lost, stolen, or damaged beyond reasonable repair as per above clauses, and may report such activity to the individual's line manager and/or Head of Department. Individuals should familiarise themselves with published guidance on reporting loss or theft available on SharePoint.

3.26. End users are not permitted to install unapproved software on devices. Requests should be made to the IT Service Desk to have additional software that is not on the approved hardware and software list installed on to a device. Any software installed must be legitimately purchased and licensed for the use made of it as per the terms of the licensing agreement,

3.27. Colleagues who have legitimate grounds for using non-standard software should complete the appropriate form on the IT Service Desk portal to request rights to do so. All requests will be assessed on a case-by-case basis; where requests are approved, end users will be held responsible for ensuring the software complies with University standards for IT security and the terms of the licensing agreement. End users will be responsible to comply with the patching policy to ensure software updates are applied in accordance with the policy for security and compliance with Cyber Essentials.

3.28. All IT assets should only be administered, managed, or maintained by ISS personnel or their nominated representative. End users should not permit anyone else access to their device in accordance with the IT Acceptable Use policy.

3.29. All IT assets capable of doing so will be enrolled in endpoint and mobile device management systems as well as cybersecurity threat and antivirus management solutions. Where these systems require software or network connectivity these must not be removed or have their configuration changed without approval from ISS. Rooted or jailbroken devices are not permitted to connect to University systems or networks.

3.30. All IT assets capable of doing so will be encrypted to prevent unauthorised access to data held or systems that can be accessed via the asset.

3.31. No data should be stored locally on an IT asset unless subject to specific terms of use outlined in 3.10. Any data that is stored locally is done so on the understanding that it may not be possible to back-up or transfer to a replacement device in the event of hardware failure or upgrade.

3.32. End users must always contact the IT Service Desk if they need to move, reassign, or return IT equipment.

3.33. All IT assets that are no longer in use must be returned to the University via the IT Service Desk for re-imaging and redeployment to ensure the device remains fit for purpose as per 3.9 as well as maintaining data compliance. This includes where the asset was purchased using research, departmental or faculty funds, or where there is little or no break in cover between a colleague leaving and a new colleague starting in the same role.

3.34. All IT assets are deployed to support the functions of a specific role at the University, whilst they may be assigned to individuals, they remain deployed to the role being carried out. If there is any change to the role or the requirement of the person carrying out the role, then the suitability of equipment provided should be reviewed in consultation with ISS.

3.35. Any person who has been provided with IT assets that are not returned to ISS when requested to do so or when no longer meeting the terms of its deployment could be subjected to disciplinary proceedings.

3.36. IT assets not returned by colleagues who have left the University will be reported to HR. These assets will be locked & wiped, and the status of these assets will be recorded as not returned in the Asset Management System.

3.37. To ensure the confidentiality of information, all IT assets that have been used to process or store personal or sensitive information will be wiped before being reissued and must go through a physical disposal and destruction process at the end of its useful life as per the IT Asset Decommissioning and Disposal Policy.

3.38. The management of IT assets must comply with this policy and the IT Acceptable Use Policy. A breach of this policy may result in user account restrictions being applied, and any device being remotely wiped, blocked from the University's network, and being prevented from using University provided services and software. A breach may also need to be dealt with in accordance with the University's disciplinary procedures.

4. Responsibilities

4.1. The Director of ISS is accountable for the implementation of this policy in the University and on a day-to-day basis the ISS department will be responsible for:

a. Coordinating IT asset audit activity including regular and no longer than quarterly inventory checks for management reporting;

b. Updating and maintaining the accuracy of the asset management system as soon as a change is made (including office moves, reports of lost or stolen equipment and disposals);

c. Identifying unreturned IT assets will be performed on a weekly basis or more frequently as required for colleagues who left the University or students who completed their studies who are no longer eligible. The Asset Management System will be updated to maintain its accuracy and ensure stolen assets are locked/wiped and do not count towards Cyber Essentials compliance;

d. Ensure that IT equipment is signed for by end users when collected from or returned to the ISS Directorate and is recorded in the Asset Management System;

e. Ensuring that all IT assets are processed, and asset tagged before they are issued to end users or entered into the ISS stores;

f. Checking IT equipment is returned in the same configuration as expected and issuing receipts upon collection from end users;

g. Administering the control and security of IT equipment held in stock for issuing and awaiting re-issue or disposal;

h. Ensuring that any IT asset that is retired is disposed of appropriately, including the removal of any sensitive or personal information on the device in line with the IT Asset Decommissioning and Disposal Policy;

i. Giving correct and appropriate advice to users on the correct handling of IT assets;

j. Reporting any incorrect disposal or misuse of an IT asset to an appropriate manager within the ISS department as soon as practicable;

k. Keeping a register of incidents for lost, stolen, and not returned IT assets will be done via the IT Service Desk incident ticketing system for monthly security reporting;

l. Enforcing lock and wipe commands in the respective mobile device management platform for unaccounted for and compromised assets;

m. Generating monthly reports of non-compliant assets against Cyber Essentials to the ISS Cyber Security Management Board; and

n. Exporting a list of stolen, lost and not returned assets to update records in other security systems for licensing purposes and false positive reporting.

4.2. End users issued with IT assets will be responsible for:

a. All IT equipment issued to them until it has been returned to ISS for redeployment or disposal;

b. Ensuring compliance with the IT Acceptable Use Policy;

c. Ensuring that IT assets are not left unattended, or stored in an unsecure location, both within and outside of the workplace;

d. Ensuring that IT assets are not moved to another location (if fixed) or transferred to another person without the express approval of ISS;

e. Ensuring that IT assets are not used or administered by those not expressly permitted to do so;

f. Familiarising themselves with the procedure for reporting the loss or theft of IT assets, which includes but is not limited to immediately reporting the loss/theft to the IT Service Desk. Prompt action for reporting lost or stolen assets is necessary as the University is required by law to report data breaches to the Information Commissioner within 72 hours of discovery;

g. Complying with any requests relating to the auditing of, or maintenance of the IT Asset, including software updates and routine security patching;

h. Undertaking security updates of non-standard and potentially non-approved software in accordance with the patching policy for security and compliance with Cyber Essentials;

i. Reporting any defects and returning IT assets immediately that are not operating normally to ISS via the IT Service Desk;

j. Returning all IT equipment to ISS upon redeployment, replacement, when it is no longer required for University business, or when the holder leaves the University;

k. Not tampering with any device in accordance with the IT Acceptable Use Policy; and

l. Requesting elevated rights where relevant and appropriate in accordance with the IT administrator policy.

4.3. Line Managers will be responsible for:

a. Ensuring that any IT assets issued to their direct reports are returned to ISS upon that colleague no longer being employed by the University, should they move into a new position at the University, or the asset is no longer required for University business. Any IT assets allocated are assigned to the role and not the individual;

b. Not withholding IT assets for redeployment to new members of staff without approval from ISS;

c. All reporting staff complying with requests from ISS relating to the auditing of, or maintenance of, IT assets that have been deployed to them; and

d. Assisting ISS with any requests or investigations relating to the misuse of IT equipment.

4.4. Personal Tutors will be responsible for:

a. Ensuring that any loaned IT assets requested for their students are recovered when no longer required to facilitate their learning requirements;

b. Reporting any missing or defective assets within their teaching environment to the IT Service Desk at the earliest opportunity as per 3.23; and

c. Working with ISS to carry out any maintenance or auditing activity required to ensure the continued use of IT assets within their teaching environment so as not to impact their student learning.

5. Compliance

5.1. Any actual or suspected breach of this policy must be reported to the Director of ISS via the most suitable channel. The Director of ISS will take appropriate action and inform the relevant internal and external authorities.

5.2. Failure to comply with this policy may be dealt with in accordance with the University's disciplinary procedures.