Keele UNIVERSITY

IT Asset Management Policy

1 INTRODUCTION

Keele University makes significant investment in the purchase and maintenance of IT hardware assets. These assets are essential for staff to be able to carry out their duties, in many cases for teaching and learning delivery but are also gateways into the university network and system. As such, an effective asset management process is vital in providing a framework to enable sufficient control over the processes necessary to manage the lifecycle of all IT equipment.

The Information and Digital Services Directorate (IDS) are the custodians of all University purchased IT assets and are responsible for the full asset management lifecycle.

1.1 Purpose

1.1.1 This policy enables IDS to ensure that all University staff understand their responsibility in the effective management of University IT hardware assets. It is designed to ensure that IT assets are:

- Managed appropriately from the point of acquisition to the time of disposal in a way that is compliant with the University's policies and regulatory obligations.
- Procured correctly in line with the University's procurement procedures and policies.
- Registered within IDS's asset management system for tracking and auditing purposes.
- Supported and maintained throughout the asset's lifecycle so that they deliver best value for the investment.
- Monitored and maintained in line with industry standards compliance such as UK GDPR, Cyber Essentials and ISO27001.
- Controlled effectively to protect the data and information that they store or transmit in accordance with the University's Information Governance policies.
- Is managed in accordance with the University's Information Security policies.
- Host and utilise software that is both appropriate and compliant with licensing agreements.
- Administrated for the identification of risk and business continuity planning.

1.2 Scope

1.2.1 This policy covers all University physical IT assets purchased by or on behalf of the University including but not limited to all desktop hardware, laptops, monitors, mobile tablets, mobile phones, digital devices, and peripherals. This policy applies to all students, staff and other associates (including sponsored IT and Honoraria, visiting and Emeritus) 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 POLICY

2.1 Management of IT Assets

2.1.1 All IT assets purchased by the University are the property of Keele University and will be deployed and utilised in a way that is deemed most effective for addressing the University's needs and objectively demonstrates value for money.

2.1.2 The budget for IT assets will be allocated and managed by the IDS Directorate on behalf of the University, except for assets purchased via research grants.

2.1.3 For compatibility and efficiency reasons, IT assets will be issued on a 'fit for purpose' basis based on predefined user roles using standard equipment. This will typically equate to one University owned laptop. Recommendations for altering the user roles and standard equipment (e.g. reasonable adjustments and specialist functions of role) will be assessed and approved by IDS.

2.1.4 Enquiries about and requests for individual IT assets must be submitted to the IDS via the IT Service Desk in accordance with current ordering processes and procedures.

2.1.5 IDS will assess requests for new and replacement IT equipment and fulfil them with standard equipment that best fits the requirement by aiming to reissue assets held in the centralised store in the first instance.

2.1.6 The procurement of IT assets must be undertaken in consultation with and carried out by IDS. IDS is responsible for engaging with the University's Procurement Team and ensuring that the best procurement practice is followed as per the University's policies and applicable legislation. In addition, all IT asset purchases will require IDS approval as part of the procurement process.

2.1.7 IDS 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.

2.1.8 IDS, in partnership with the Procurement Team are responsible for identifying and managing sources and channels for the purchase of IT assets, utilising existing framework agreements whenever possible.

2.1.9 All IT assets (excluding low-value peripheral items, e.g. keyboards, mice, etc.) will be registered in the asset management system and be asset tagged before being issued or put into use.

2.1.10 All IT assets must be assigned to individual users or to a department who will always be expected to take all reasonable steps to ensure the IT assets' care and security whether they are in use, storage or movement.

2.1.11 Information about all IT assets will be held in the asset management system, which will be maintained by IDS, to enable the assets to be tracked, managed and audited throughout their entire lifecycle.

2.1.12 All IT equipment purchased by the University will be stored in centralised asset management stores managed by the IDS when they have not been issued or are not in use.

2.1.13 IT assets will be adequately administered and maintained by IT to ensure they remain fit for purpose and compliant with the licenced conditions of use during their entire lifecycle.

2.1.14 Individual users or departments will take all reasonable steps for protecting the IT assets that have been assigned to them against physical or financial loss whether by theft, mishandling or accidental damage, by using appropriate physical security measures.

2.1.15 Individual users or departments will comply with all IT requests for remote or physical access to IT assets in support of technical fault resolution, maintenance, cyber security investigations, and investigations into suspected breaches of university policies.

2.1.16 End users are not allowed to install software on university devices that is not available via the Company Portal app (Windows) or Keele Self Service app (MacOS) without approval. Requests must be made to the IT Service Desk to have additional software reviewed for approval before being installed. Any software installed must be legitimately purchased and licensed for its purpose of use.

2.1.17 Users must always contact the IT Service Desk if they need to move non-portable IT equipment (e.g. Desktops), reassign IT equipment to another person or return IT equipment.

2.1.18 All IT assets that are no longer in use must be returned to the University via the IT Service Desk for redeployment. This includes where the asset was purchased using research, departmental or institute funds.

2.1.19 To ensure the confidentiality of information, any IT asset that has been used to process or store data will be erased before being reissued and must go through a physical disposal and destruction process at the end of its useful life as defined by the Information Security Policy.

2.1.20 The management of IT assets must comply with this policy. Breach of this policy may result in any device being remotely erased, blocked from the University's network and being prevented from using University provided services and software. A breach may also be considered a disciplinary offence.

2.2 New IT Assets

2.2.1 New IT assets should only be required:

- When an existing device has come to end-of-life as defined and assessed by IDS and as highlighted in the University's asset management system.
- When new posts are created requiring an IT asset.
- When assistive reasonable adjustments are considered through Occupational Health recommendations.
- When new requirements for the allocation of IT assets to students are identified.

- When new programmes are initiated or existing programmes updated that require IT assets for delivery, such as teaching labs etc.
- When research funding has been allocated that includes the purchase of IT assets.

2.2.2 All new assets should be purchased according to the University procurement procedure, regulations and framework agreements and appropriate asset specifications will be defined by IDS in alignment with requirements and, where appropriate, job roles.

2.2.3 All new IT assets are recorded in the University's asset management system. This system contains key information that facilitates effective management of the asset. The main user of the asset will be recorded but only in terms of information that will allow identification of that user for use in management and support of the asset.

2.3 Asset Changes and Replacements

2.3.1 If an asset becomes faulty or broken and cannot be repaired by the University's supplier, a replacement device is issued.

2.3.2 For University owned IT assets, if an upgrade was required to replace faulty parts or increase performance then these changes are updated and reflected in the University's asset management system.

2.4 Returning Assets

2.4.1 All IT assets must be returned to the Service Desk:

- When a member of staff is leaving the employment of the University.
- When a research-funded project comes to an end.
- When a student issued with IT equipment leaves the University.
- When the engagement of a third-party who has been issued with IT equipment finishes or the equipment is no longer required.

2.4.2 Staff termination dates for employees will be flagged to IDS from within the HR system.

2.4.3 All IT assets must be returned on, or before, the last day of employment or contracted engagement with the university unless prior approval is agreed with IDS via the Service Desk.

2.4.4 Students must return all IT assets after confirmation and prior to graduation or on termination of their studies.

2.4.5 When assets are returned, they will be checked in to the asset management system and booked back in to the pool for re-allocation or disposed of.

2.4.6 Should devices not be returned as outlined above, appropriate university and legal procedures for recovery of university owned assets will be explored.

2.5 Disposal of Assets

2.5.1 All IT asset disposal must be requested through the IT Service Desk regardless of item age or condition.

2.5.2 Assets will be assessed as to their suitability for redeployment or destruction and recycling in line with the Information Security Policy.

2.5.3 The disposal or redeployment of assets will be recorded in the asset management system.

2.5.4 Assets will be disposed of inline with industry standards to comply with UK government waste electrical and electronic equipment (WEEE) guidelines.

2.6 Lost or Damaged Assets

2.6.1 If an asset is lost, stolen or damaged, it must be reported to the IT Service Desk as soon as possible.

2.6.2 The loss of all IT assets capable of storing or accessing University data must be reported as a Data Breach via the Information Governance webpages in line with the Information Security Policy and Data Protection Policy.

2.6.3 Damaged assets may need to be assessed by IT for safety and repair or replacement.

2.7 International Travel with University IT Assets

2.7.1 All users intending to travel internationally with university owned IT assets are required to complete a form via the IT Service Desk. This form will help users to identify any potential risks they may need to be aware of while ensuring the safety of Keele data, systems and equipment in line with Keele Policies and UK laws.

2.7.2 This data will be used by Keele's Cyber Security team when responding to cyber incidents and reports of suspicious or unusual international access to Keele systems.

3 ROLES AND RESPONSIBILITIES

3.1 Roles

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

3.2 Responsibility

- The Head of Enterprise Services is responsible for reviewing and maintaining this policy and for its application in operational terms.
- Line Managers are responsible for ensuring employees understand this policy and that the processes outlined in the supporting procedures document are completed including the return of all IT assets when an employee leaves the employ of the University.
- Sponsors are responsible for ensuring third parties understand this policy and that the processes outlined in the supporting procedures document are completed including the return of all IT assets when a sponsor's engagement with the University is concluded.

- Supervisors / Academic Mentors are responsible for ensuring students issued with IT assets understand this policy and that the processes outlined in the supporting procedures document are completed including the return of all IT assets prior to a student graduating or leaving the University.

4 RELATED POLICIES AND PROCEDURES

4.1 Policies

- IT Acceptable Use Policy
- Information Security Policy
- Data Protection Policy
- Electrical Safety Policy

4.2 Procedures

- IT Asset Management Procedures
- Procurement Procedure
- Leavers Procedure

5 REVIEW, APPROVAL & PUBLICATION

5.1.1 This policy will be reviewed every three years by the Head of Enterprise Services, with approval from the Director of IT and Chief Information Officer, and final sign off from UEC.

5.1.2 This review will be uploaded to Policy Zone to update the current policy which is in the same location.

https://www.keele.ac.uk/policyzone/data/itassetmanagementpolicy

6 DOCUMENT CONTROL INFORMATION

Document Name	IT Asset Management Policy
Owner	Head of Enterprise Services
Version Number	1.0
Equality Analysis Form Submission Date	24 February 2025
Approval Date	11 March 2025
Approved By	University Executive Committee
Date of Commencement	17 March 2025
Date of Last Review	11 March 2025
Date for Next Review	11 March 2028
Related University Policy Documents	• IT Acceptable Use Policy • Information Security Policy • Data Protection Policy • Electrical Safety Policy
For Office Use – Keywords for search function	