

Hardware Asset Management Policy

UNIVERSITY OF WOLVERHAMPTON

INDEX

1. Introduction
2. Purpose
3. Principles
4. Scope
5. Definitions
6. Roles and Responsibilities
7. Policy (Main Body with Associated Headings)
8. Data Protection Requirements
9. Training
10. Exceptions
11. Amendments
12. Information and Resources
13. Contact

POLICY

1. Introduction

The University of Wolverhampton relies on hardware assets to support teaching, research, professional services and the secure delivery of digital services across the institution. These assets include end-user devices and other hardware used to access, process, store or support University systems and information.

To support accountability, security, value for money and effective lifecycle management, hardware assets must be managed through clear governance arrangements and consistent control requirements. This policy provides the University's overarching framework for the management of hardware assets and should be read alongside associated procedures, standards and related University policies.

2. Purpose

This policy sets out the University's requirements for the governance and lifecycle management of hardware assets used for university purposes. It is intended to support security, accountability, compliance, value for money and effective service delivery across teaching, research and corporate services.

The policy establishes the minimum control requirements for how hardware is requested, approved, acquired, issued, recorded, supported, returned, reused, refreshed and retired across the University. It is supported by related procedures, service arrangements and technical standards, which set out the operating detail.

3. Principles

The University will maintain central oversight of managed hardware through designated systems, records and processes. Hardware should normally be drawn from approved, supportable and secure University procured devices unless an agreed exception applies.

Users are expected to take reasonable care of hardware issued to them and to return it when required. Line managers, budget holders and relevant support functions must co-operate to support issue, recovery, refresh and return controls.

The University should seek to reduce ghost assets, informal local storage and inaccurate records by using central recovery, reassignment and disposal routes.

4. Scope

This policy applies to:

- University-owned end-user devices, including laptops, desktops, tablets and mobile phones including laptops acquired for the University’s student loan system
- managed server and other hardware assets where the University records and governs them

through approved asset management processes
- tracked monitors and other peripheral equipment where the University has chosen to manage or record those items through its approved processes
- locally funded or specialist hardware used for university purposes where it connects to university services, holds University data, or is otherwise brought within university governance
- asset records, issue information, return information, disposal evidence and related lifecycle documentation held by or on behalf of the University

This policy applies to the University's core teaching, research and professional services activities. Separate legal entities or University-associated entities may be out of scope unless expressly brought within these arrangements.

The policy does not replace information security, acceptable use, procurement, mobile device or bring-your-own-device requirements. Those policies continue to apply alongside this policy where relevant.

5. Definitions

- **Hardware asset:** A physical device or related item used for university purposes and managed within the scope of this policy.

- **Managed hardware:** Hardware governed through university processes or Digital Services controls.

- **Ghost asset:** A device recorded or believed to exist but not readily locatable, accountable for, or reflected accurately in current records. These devices are not procured or managed by Digital Services.

- **Central return:** Return of hardware into the approved University process so that records, reuse, sanitisation and disposal can be managed properly.

- **User:** Any individual authorised to use University hardware, including employees, students, researchers, visiting lecturers, honorary staff, casual and fixed-term staff, contractors, agency workers and other approved third parties.

- **End-user device:** A hardware device issued to, used by, or made available for use by an individual, team or location to access University systems, services or information, including laptops, desktops, tablets and mobile phones.

- **Peripheral:** An accessory or supporting hardware item used with an end-user device or other managed hardware, including monitors, docking stations, keyboards, mice, headsets and similar equipment where the University chooses to manage or record those items.

- **Reasonable adjustment:** A change to equipment, provision or working arrangements made to support a disabled member of staff or other individual with an accessibility requirement, in line

with the University's duties under the Equality Act 2010.

6. Roles and Responsibilities

6.1 Digital Services

Digital Services is responsible for operating the University's hardware asset management controls and supporting procedures. This includes maintaining designated asset records for managed hardware within scope; issuing, recovering, reassigning, refreshing and retiring hardware through approved processes; ensuring secure wiping, sanitisation, disposal or recycling through approved routes; maintaining disposal evidence; and supporting reporting for management, governance and audit purposes.

6.2 Line Managers and Budget Holders

Line managers and budget holders must ensure that staff follow the correct route for requesting, returning and accounting for university hardware. They must support recovery during role changes, departures, transfers or other changes in circumstance, and they must not retain returned hardware locally outside the approved process.

6.3 Users

Users must take reasonable care of University hardware issued to them, must not pass it to another user outside approved processes, and must return it when requested, on change of role, or on leaving the University.

6.4 Human Resources, Estates, Procurement and Other Supporting Functions

Supporting functions should co-operate where hardware return, storage, movement, procurement or disposal forms part of wider University controls. They should work with Digital Services and management teams where return, accountability or disposal issues arise.

7. Policy

7.1 Policy Statement

University-owned hardware remains University property regardless of the budget, School, Faculty, Department, project or funding source from which it was acquired. Hardware within scope must be requested, issued, recorded, recovered, reused and retired through approved University routes. Hardware must not be informally retained, exchanged, stored, passed between users or disposed of outside approved processes. Returned hardware should be assessed for reuse or redeployment where appropriate before disposal is undertaken.

Disposal of hardware must be secure, auditable and capable of being evidenced within university records. Hardware connected to the University environment must also meet relevant university requirements for management, security and support.

7.2 Hardware Lifecycle Requirements

7.2.1 Acquisition and Standard Provision

Hardware should normally be acquired through approved suppliers and standard university routes. Standard device provision should be used wherever suitable. Requests outside standard provision

should follow an approved exception process that considers business need, supportability, security, compatibility and cost.

7.2.2 Asset Recording and Issue

Managed hardware should be recorded in designated University asset systems or registers. Where equipment is issued to an individual, team or location, the University should maintain sufficient information to support accountability, recovery and lifecycle management.

7.2.3 Use, Movement and Reallocation

Hardware should not be informally transferred between users, teams or locations without the relevant update to university records or process. Devices returned to Digital Services should be assessed for continued use, reimaging or reassignment before new equipment is issued where this is appropriate and practical.

7.2.4 Loss, Theft and Damage

Loss, theft or damage to university hardware must be reported promptly through the appropriate University route and in line with relevant University procedures. Digital Services and relevant stakeholders will manage the response in accordance with applicable recovery, replacement, record update, information security and escalation requirements.

7.2.5 Refresh and Retirement

Hardware should be reviewed for continued suitability, supportability and reuse. When hardware reaches end of life, becomes uneconomic to support, or is no longer required, it should be retired through approved routes. The University should continue to improve visibility of refresh requirements, unsupported devices and other priority lifecycle issues through management information and review.

7.3 Joiners, Movers and Leavers

Hardware issued for University business must be recoverable at the point a user changes role, no longer requires the equipment, or leaves the University. Hardware must be returned to Digital Services, or another formally approved return point defined by Digital Services, before or on the final working day unless alternative arrangements are agreed.

The University should support joined-up processes to identify hardware assigned to a user or location in advance of departure or role change, with follow-up and escalation where assets are not returned. Return to a line manager does not remove the requirement for the item to be returned through the approved University process and reflected in central records.

Where a user moves between roles, teams, Schools, Faculties, or departments within the university, the hardware retained by the user should be reviewed for continued suitability, and data removed where it is not pertinent to the move. Asset records should be updated to reflect the new role, and department, and that any equipment no longer required is returned to Digital Services. Hardware should not be informally retained by the user, or the releasing or receiving department without an updated asset record. Internal movement of hardware between teams or locations does not remove the requirement for accurate central records.

Where University hardware has been issued to a contractor, agency worker, honorary, visiting or non-employee, the engaging manager or sponsor is responsible for ensuring that the equipment is returned to Digital Services at the end of the engagement, contract, secondment or visit, or where the engagement is terminated, expires, or is otherwise concluded. The standard leaver routes that apply to employees may not be triggered automatically for these individuals, and proactive return arrangements should be put in place at the point the engagement is set up.

The university reserves the right to assess and recover the current market value, minus costs for reasonable wear and tear, for any unreturned, lost or damaged hardware. Failure to return equipment upon termination of employment for staff, or upon request for all Users, may result in legal action or deduction from final wages where it is permitted by law and appropriate.

7.4 Central Return, Disposal and Evidence

Hardware no longer required must be returned through the approved route so that the University can assess reuse, remove data where appropriate, update asset records and maintain an auditable disposal trail. Digital Services should be engaged before destruction or disposal of hardware within scope.

Disposal records should identify, as far as reasonably practicable, the specific assets sent for disposal or destruction. Disposal evidence should be retained in line with university record-keeping requirements and linked back to the relevant asset record where possible. Working or reusable devices should not be destroyed without appropriate review through the approved process.

Data held on returned hardware must be removed using approved sanitization methods appropriate to the device type and the sensitivity of the information held, and consistent with the university's Data Protection obligations under the Data Protection Act 2018. Where physical destruction is required, it should be undertaken by an approved supplier capable of providing a Certificate of Destruction, which is in addition to any WEEE transfer note.

Records of sanitization, destruction an onward routing of hardware, including reuse, refurbishment, donation or recycling, should be retained have evident chain of custody for the device from issue to final disposal. Asset records should be updated to reflect the disposal outcome so that the device is not subsequently reported as active, missing or unaccounted for in the IT Asset Management system, or management information audit reporting.

7.5 Locally Funded and Specialist Hardware

The University recognises that some specialist teaching, research or project activity may require hardware outside standard provision. This does not remove the requirement to comply with university policy. Locally funded hardware must not be treated as outside policy simply because it was purchased from a local budget. Hardware acquired through research grants, project funding or similar local arrangements remains University property unless expressly agreed otherwise through formal University arrangements, and must be managed, returned or disposed of in line with this policy when the relevant activity or funding period ends.

Where locally funded hardware is to be connected to university services, used with university data or supported by Digital Services, it must meet applicable approval, security and support requirements. Hardware that is not approved or not managed to the required standard may be restricted from university services or support. Specialist or exceptional arrangements should be documented through the relevant approval or exception process.

7.6 Accessibility and Reasonable Adjustments

The University recognises its duties under the Equality Act 2010 to make reasonable adjustments for staff with disabilities or accessibility requirements. Hardware should be provided in a manner that supports inclusive working and removes barriers to participation in university activity.

Where a member of staff requires a laptop or other hardware that differs from standard provision in order to meet an accessibility requirement, the request should be made through the approved university route, supported as appropriate by Human Resources, Occupational Health, the staff member's line manager and any relevant workplace adjustment assessment, including an Access to Work assessment where applicable.

Digital Services should work with Human Resources, Occupational Health, and the requesting department to identify suitable, supportable equipment, including assistive technologies, alternative form factors, or additional peripheral equipment, taking into account the business need, security, supportability and costs. The cost of adjustment related hardware is normally met by the School, Faculty or department in which the member of staff is employed, with Digital Services advising on appropriate options and supportability. Approved adjustments should be recorded in line with data protection and confidentiality requirements, and personal medial information should not be retained within Asset records.

Hardware issued under these arrangements remains within the scope of this policy and is subject to the same lifecycle, return and disposal requirements as other university hardware, recognizing that continuity of provision and timely replacement maybe a particular consideration where reasonable adjustments are in place.

7.7 Governance, Records and Reporting

The University will maintain management information to support effective hardware asset management. This should include regular reporting or review of matters such as unsupported devices, missing or unreturned assets, disposal activity, refresh needs, exceptions and other priority issues.

Asset records, issue information, return status, disposal evidence and other supporting documentation must be retained in the designated University record or repository so that the University can evidence custody, support recovery activity and inform planning. The University should continue to improve the completeness and consistency of its central hardware records across managed hardware and, where possible, in relation to locally procured or decentralised hardware that falls within scope.

7.8 Sustainability and Environmental Responsibility

The University is committed to managing its hardware estate in a manner that supports its wider environmental obligations and net zero commitments. Hardware decisions should take account of whole-life impact, including responsible procurement, energy efficiency in use, extended useful life, reuse, refurbishment and end-of-life treatment.

Where practical and supportable, hardware should be acquired from approved suppliers that demonstrate responsible sourcing and recognized environmental standards. Devices should normally be retained in service for their full, supportable life, with refresh decisions informed by suitability, security and supportability rather than age alone.

Returned hardware should be assessed for reuse, redeployment or refurbishment through approved routes before disposal is considered. Where disposal is necessary, it must be undertaken through routes that meet Waste Electrical and Electronic Equipment (WEEE) requirements, maintain data security, and provide auditable evidence of environmentally responsible treatment.

Digital Services should support reporting on hardware sustainability matters, including estate refresh patterns, reuse and disposal volumes, and the contribution of hardware lifecycle activity to the university's wider environmental and net zero reporting.

7.9 Disclosure and Compliance

Failure to comply with this policy may result in hardware being recovered, access being restricted, support being refused, or further action being taken under relevant University procedures, contractual arrangements, disciplinary processes or other governance routes, depending on the circumstances.

Any known or suspected breach of this policy should be reported to Digital Services as soon as possible, using the appropriate University reporting route via ITSupport@wlv.ac.uk

8. Data Protection Requirements

When personal data is expected to be used under this policy, staff must adhere to applicable data protection laws. These are outlined in the University's Data Protection Policy and related policies (https://www.wlv.ac.uk/about-us/corporate-information/wlv-policies/). Any use of personal data should be detailed in the relevant privacy notice and processed in accordance with all data protection principles.

For processing activities that may carry high risk; completion of a Data Protection Impact Assessment (DPIA) may be required. This is determined by answering a series of screening questions included in the DPIA template. The Data Protection Team is available to provide assistance and guidance with any part of this process, please contact them via email: dataprotection@wlv.ac.uk.

Please note that whilst the Data Protection Act does not cover aggregate data, it must be ensured that small numbers held within aggregate data sets do not inadvertently identify individuals.

9. Training

Training is equipping staff, students (and others where appropriate) with the relevant skills required for/with this Hardware Asset Management Policy Training relating to this policy and briefing will be made available in a range of formats according to the needs of the trainee and different groups of staff, students and others.

The University will provide appropriate awareness, guidance and supporting materials to help relevant staff understand and comply with this policy.

This may include guidance for Digital Services, budget holders, managers, requesters and users on approved software routes, standard provision, exception handling, lifecycle controls, and associated procedures or standards issued under this policy.

10. Exceptions

Exceptions to this policy must be formally considered and approved through the relevant University route. Any approved exception must be documented together with its rationale, scope, duration, review point and any conditions or compensating controls that apply.

11. Amendments

This Policy was approved by the University's Executive Board on 28 July 2026. The University may change this Policy at any time, and where appropriate. Where a policy is not due for review, but is found to require updating, it will remain published, unless the reasons for review render it obsolete.

12. Information and Resources

This policy should be read in conjunction with the following policies and guidance:

12.1 Digital Services

- IT Acceptable Use Policy: https://www.wlv.ac.uk/about-us/corporate-information/wlv-policies/it-acceptable-use-policy/

- Information Security Policy: https://www.wlv.ac.uk/about-us/corporate-information/wlv-policies/information-security-policy-/

- Bring Your Own Device Policy: https://www.wlv.ac.uk/about-us/corporate-information/wlv-policies/bring-your-own-device-byod-policy/

12.2 Procurement

- Procurement Policy: https://www.wlv.ac.uk/about-us/corporate-information/wlv-policies/procurement-policy-and-procedures/

12.3 Data Protection

- Data Protection Policy: https://www.wlv.ac.uk/about-us/corporate-information/wlv-policies/data-protection-policy/

- Data Protection Act 2018: https://www.legislation.gov.uk/ukpga/2018/12/contents

12.4 Equality

- Equality Act 2010: https://www.legislation.gov.uk/ukpga/2010/15/contents

13. Contact

For guidance, support and queries regarding this policy please contact Thomas McKenna, IT Asset Manager, Digital Services.
Email: Thomas.McKenna@wlv.ac.uk

For general queries, please contact the Corporate Compliance Team via email: compliance@wlv.ac.uk.

VERSION	1	**AUTHOR OWNER**	Thomas McKenna Digital Services
Approved Date	28 July 2026	**Approved By**	University Executive Board
Review Date	28 July 2029		