Software 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 software assets to support teaching, research, professional services and the effective operation of its wider digital environment. Software may be acquired and used through a range of routes, including centrally managed provision, locally funded arrangements, hosted services and subscription-based models.

To support security, compliance, value for money and effective service delivery, software assets must be subject to clear governance and lifecycle control. This policy provides the University's overarching framework for the management of software 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 software assets used for university purposes. It is intended to support security, accountability, compliance, value for money and effective service delivery across teaching, research and professional services.

The policy establishes the minimum control requirements for how software is requested, approved, acquired, deployed, recorded, reviewed, reallocated, renewed and retired across the University. It is supported by related procedures, service arrangements and technical standards, which set out the operating detail.

3. Principles

Software that has been approved through the University’s relevant governance, procurement and Digital Services processes, or identified as part of the University’s standard provision, should be used wherever suitable to support consistency, supportability and value for money. Where the University already holds suitable entitlement or support capability, such software should normally be used in preference to duplicate or alternative products.

Software decisions should take account of business need, educational or research requirement, information security, data protection, technical fit, support implications, total cost and contractual terms. Local funding does not remove the requirement to follow University policy where software is used for university purposes or interacts with university systems, devices or data.

Where a request falls outside standard provision, an exception route may be used, but the business need and associated risks must be considered and approved. Requests approved through an exception route will still be subject to the University’s software lifecycle controls. Software lifecycle controls should support visibility over allocation, utilisation, renewals, deprovisioning and reclaim opportunities.

4. Scope

This policy applies to:

- Software used for university business, teaching, research or administration
- Software installed on university-managed devices, servers or other managed environments
- Browser-based, hosted and subscription services, including Software as a Service
- Software procured centrally by Digital Services and software procured locally by Schools, Faculties, Departments, research teams or project budgets used for university purposes
- Software contracts, subscriptions, licence records, renewals and related usage information held by or on behalf of the University
- Freeware and educationally licensed software where the University relies on terms of use or licence conditions to permit use
- Open-source software is also within scope where its use for university purposes requires review of licence terms, attribution, support, security or other legal or operational considerations.

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.

This policy does not set the University's detailed position on enterprise AI governance, cloud financial management or wider infrastructure strategy. Where those areas overlap with software use, they will continue to be managed through relevant University governance, information security and Digital Services arrangements until further policy or standard is issued.

Software incorporating artificial intelligence or generative AI capabilities, whether as a primary function or an embedded feature, falls within the scope of this policy, where used for university purposes. The acquisition, approval, deployment, recording and lifecycle management of such software must follow the routes set out in this policy, including where AI features are introduced through updates, add-ons or changes to existing products. Wider matters relating to the responsible and ethical use of artificial intelligence, including permitted use cases, data handling, and governance, are managed through the university’s separate governance arrangements, which should be read alongside this policy.

4.1 Out of Scope

The following are explicitly out of scope for this policy

- Electronic books (ebooks), electronic journals, online databases, digital publications, and other library information/content resources that are acquired, licensed, or managed by the university Library Services.
- Library resource licenses that govern access to published academic content rather that the use of software.
- Printed books, journals, and other non-software information resources.
- Research datasets and digital content that do not constitute software or require software

license.

These resources are governed by the University Library Services, publisher license agreements, copyright legislation and other relevant institutional policies where available.

5. Definitions

- **Software asset**: Any software product, application, subscription, hosted service, licence or related entitlement used for university purposes.
- **Software as a Service (SaaS)**: Software accessed as a hosted or browser-based service rather than installed and run solely on local infrastructure.
- **Standard software**: Software that the University has approved for general or defined use and is prepared to govern and support through normal arrangements.
- **Exception**: An approved departure from standard provision or normal policy requirements, subject to conditions and review.
- **User**: Any individual, including current employees, students, researchers, visiting lecturers, honorary staff, casual and fixed-term staff, contractors, agency workers and other approved third parties, where a license authorises the use of university acquired software, and SaaS.

6. Roles and Responsibilities

6.1 Digital Services

Digital Services is responsible for operating the University's software asset management controls and supporting procedures. This includes reviewing software requests, where required, for technical fit, deployment method, support route, licence implications and lifecycle management; maintaining central software records within designated systems; supporting reclaim, reassignment, removal and retirement; and operating the relevant exception, escalation and review processes under this policy.

6.2 Procurement Legal Services and Other Relevant Functions

Procurement advises on applicable routes to market, tendering requirements and related purchasing activity in line with university procurement requirements.

Legal Services may be engaged, where required, to support contractual and end user licence agreement review.

Digital Services, Procurement, Legal Services, budget holders and other relevant stakeholders must work together, as appropriate, on software acquisition, contracting, renewal activity and supplier engagement, according to the nature, value and intended use of the software concerned.

6.3 Budget Holders, Schools, Faculties, Departments and Research Teams

Budget holders and local teams must raise software requirements through the appropriate University route, avoid duplicate, unsupported or unapproved purchases, co-operate with software review and renewal activity, and ensure that locally funded software used for university purposes is declared or reviewed where required by this policy.

6.4 Users

Users must only use software in line with this policy and associated University policies. They must not install, subscribe to or use software for university business outside approved routes, and they must co-operate with reassignment, removal, deprovisioning, audit and review activities.

7. Policy

7.1 Policy Statement

Software must be requested, assessed, approved, acquired, deployed and retired through defined University routes. Software must not be introduced into the University environment, or used for university business, outside approved processes simply because it is free, locally funded, browser-based or easy to obtain.

The University will maintain a central record, as far as reasonably practicable, of software within scope together with the key contract, renewal and licence information needed to manage compliance, support and decision-making. Software used on university-managed devices or with university data must be capable of being governed, supported and, where appropriate, removed or reassigned.

The University will seek to reuse, reassign, rationalise or retire software where this is appropriate in order to reduce cost, duplication and risk. Non-compliance with this policy may result in software being refused, blocked, removed, reallocated or escalated under relevant University procedures.

7.2 Software Lifecycle Requirements

7.2.1 Request and Approval

Software requests must be raised through approved channels. Requests are assessed against business need, existing provision, supportability, information security and data considerations, licensing requirements, contractual terms, cost and the availability of suitable standard software. Requests outside standard provision should follow a defined exception route.

7.2.2 Acquisition and Contracting

Software procurement must follow University procurement requirements. Personal subscriptions, reimbursement routes and other informal arrangements must not be used for subsequent University use. Contractual, legal and licensing review must take place through the appropriate University route where required. Software contracts, renewals and entitlement information within scope must be recorded in designated University records. Key software use rights, restrictions and obligations must also be identified, understood and retained where relevant, including matters such as permitted users, named-user or concurrent licensing, virtualisation rights, cloud-hosted use rights, geographic or entity restrictions, educational use rights, research use rights, and any other material limitations or conditions that may affect deployment, allocation, renewal or continued use.

7.2.3 Deployment and Use

Software on University-managed devices or managed environments should be deployed or enabled through approved Digital Services processes unless a formally approved alternative route applies. Digital Services may refuse installation or use where software is not appropriately approved, cannot be supported, is not compatible with the University environment, or presents unacceptable risk.

7.2.4 Monitoring, Review and Reallocation

The University will actively monitor software deployment and usage information, where lawful and proportionate, to maintain records, manage licences, identify duplication or under-use and support renewal decisions. This may include the use of approved technical discovery, inventory and other monitoring mechanisms for installed, browser-based, hosted and Software as a Service solution within scope. Software that is no longer required should be removed, deprovisioned or reassigned.

7.2.5 Renewal and Retirement

Software renewals should be reviewed before commitment is made, including consideration of need, usage, available alternatives, contractual position and whether the software remains suitable and supportable. When software is retired or no longer required, relevant licences, accounts, access and records should be updated promptly.

7.2.6 End-of Life and Unsupported Software

The university will identify software that has reached, or is approaching the end of vendor support, and will manage the associated risks through upgrade, replacement, removal or formal exception with compensating controls. Continued use of unsupported software for university purposes must not occur outside an approved exception, given the information security, compliance and supportability implications. The identification of end-of-life and unsupported software will form part of our routine software asset management reporting.

7.3 Joiners, Movers and Leavers

Software allocation and deprovisioning will form part of the University's joiner, mover and leaver controls. Where a user changes role, leaves the University, or no longer requires specific software, access and licence assignment should be reviewed and updated promptly.

The University will maintain appropriate processes to ensure that software allocated to users or devices can be identified, reviewed, reclaimed, reassigned or removed where appropriate. This is particularly important where software is subscription-based or subject to renewal, so that software no longer required is deprovisioned promptly and unnecessary ongoing cost or automatic renewal is avoided.

7.4 Locally Procured and Non-Standard Software

The University recognises that specialist teaching, research or project needs may arise outside standard provision. This does not remove the requirement to comply with university policy. Software bought locally or obtained directly by a School, Faculty, Department or project team must not be treated as outside policy simply because it is not paid for by Digital Services.

Software bought or obtained outside approved routes must not be installed on university-managed devices without approval. Browser-based or Software as a Service solution used for university purposes remain in scope where they process University data, use University accounts, or create support, licensing, information security or contractual obligations. This includes free, freemium and trial services where a university email address, University account or University data is used to access, register for or consume the service. Software that cannot be governed or supported to the required standard may be restricted, removed or refused.

7.5 Software as a Service

Software as a Service (SaaS) introduces specific lifecycle considerations that differ from installed software, including identity-based licensing, usage-based charging, automatic renewal terms, data residency and the time-critical nature of deprovisioning when users leave or change role. SaaS within scope must be acquired through approved University routes, recorded in designated University systems, and reviewed in advance of renewal commitment dates. Identity, access and licence assignment for SaaS must align with the university joiner, mover and leaver controls, with deprovisioning completed promptly when entitlement is no longer justified. Contractual provisions covering data return, data deletion and exit on termination are considered factors as part of the acquisition and renewal review.

7.6 Governance, Records and Reporting

The University will maintain management information to support effective software asset management. This should include regular reporting or review of matters such as software within scope, unsupported software, licence utilisation, renewals, reallocation opportunities, exceptions and other priority risks or control issues.

Records relating to software requests, approvals, contracts, renewals, entitlement information, deployment, reassignment and retirement must be retained in the designated University record or repository so that the University can evidence its position and support informed decision-making. Approved exceptions must also be documented together with any conditions, review points or compensating controls.

7.7 Accessibility and Workplace Adjustment Software

The University is committed to meeting its duties under the Equality Act 2010, including the provision of reasonable adjustments for staff with disabilities or other accessibility requirements. Where software is recommended as part of a workplace adjustment, for example, through Human Resources, Occupational Health, or an external assessment such as Access to Work. It will be considered through a supported route that takes account of the individual’s needs alongside the University’s information security, licensing and support requirements.

7.8 Sustainability

The University recognises that decisions about software acquisition, deployment and retirement contribute to its wider environmental and social responsibilities, including its commitments on carbon reduction, responsible procurement and ethical supply chains.

Where reasonably practicable, software decisions made under this policy should take account of sustainability considerations alongside business need, cost and technical fit. This may include the rationalisation of duplicate or under-utilised licences to reduce unnecessary digital consumption, consideration of supplier sustainability credentials and reporting where relevant during procurement and renewal, and the avoidance of software that requires hardware replacement where existing university-managed devices remain fit for purpose.

Digital Services will work with suppliers to support visibility over the environment impact of software and hosted services within scope, where information is reasonably available, and to align software lifecycle decision with the university's sustainability strategy and related commitments.

7.9 Disclosure and Compliance

Failure to comply with this policy may result in software being refused, removed, blocked, deprovisioned or escalated 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, with the relevant skills required for effective IT Asset Management, to be trained in asset lifecycle processes, licensing compliance, governance and the use of supporting tools.

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

- 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 and Procedures: 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**	Nick Gorman – Director of Digital Services
Approved Date	28 July 2026	**Approved By**	University Executive Board
Review Date	28 July 2029		