Software Management Policy

1. Purpose

1.1 The purpose of this Policy is to ensure that the University meets its legal and contractual obligations, obtains value for money and operates effectively and securely in its licensing, procurement and management of software.

This Policy applies to any staff or students involved in the specification, acquisition, installation, use and maintenance of software and all software used whether purchased outright, leased, renewed, hosted via a third party (Software as a Service), shareware or freeware.

Infringements of this Policy may lead to disciplinary action against individuals under the University's disciplinary procedures and may result in legal action and criminal proceedings against the University and/or individuals.

1.2 Definitions

a) Software management relates to any procurement, development, installation, regulation, maintenance or removal of software that takes place on University-owned computers or computers permitted connection to University networks.

b) Software relates to any application that is installed on your local device or accessed through web browser that requires any type of login credentials or profile to be created in order to use services.

c) Computers refer to all end user computing devices including smartphones, tablets and servers, as well as desktop and laptop devices.

d) Conditions of Use refers to the specific conditions stipulated in a license agreement.

2. Software Management Principles

2.1 All software (including operating systems and applications) must be actively managed.

2.2 No software or application to which licence conditions or Conditions of Use pertain, shall be made available on any University computer or IT system, for which a prior licence has not been procured or properly acquired or renewed. Software that is beyond its end of extended support (where security fixes are no longer available) must be replaced.

2.3 The Conditions of Use of any such product or application shall be adhered to subsequent to the software being made available for use. Where any such licence restricts the use of the software to a limited number of users, such limits will be strictly adhered to.

2.4 There must be an identifiable individual or organisation taking current responsibility for every item of software deployed.

2.5 In all cases IT Services is responsible for maintenance, acquisition renewal or update of software products and applications it will maintain and manage appropriate License and Conditions of Use compliance as far as possible.

2.6 In all cases where local departments (or Schools) have to procure specialised or limited software products for local deployment, a request must be made to the Software Licensing Department.

2.7 In general, site licensed software provides for use on campus by staff and students for academic, research and/or teaching and in some instances, such as Microsoft, the University's business and administration functions. Users should verify, through IT Services, that software intended to support consultancy or other external or non-academic work is permitted under the terms of the product license. Where license conditions restrict such anticipated use, IT Services will use best endeavours to identify suitable alternatives.

2.8 Individuals who have elected to be responsible for the administration of their School's specialist software applications shall be responsible to the Head of Department/Head of School and IT Services for software licence compliance in relation to those installed applications and machines.

2.9 Those responsible for software must monitor relevant sources of information which may alert them to a need to act in relation to new security vulnerabilities and available fixes.

2.10 Staff involved in managing software are responsible for ensuring the ongoing security of their software and must apply security patches in a timely manner (high-risk or critical security updates for operating systems or firmware must be installed within 14 days of release, or other compensatory control measures taken to mitigate risk, such as isolating, blacklisting or removing the software).

2.11 Staff involved in managing software should have experience, training or qualification commensurate with the importance of the software and risk levels involved. At the minimum all staff involved must be aware of, and proactive in managing, information security-related risks associated with software. University departments are expected to support this policy by ensuring that permission and responsibility for systems and software management is delegated accordingly.

2.12 University software management procedures must incorporate measures for controlling these information security risks:

a) Illegal use of software

b) Use of software for illegal purposes

c) Software copyright infringement

d) Inadequate control over data access by software

e) Insecure software design, configuration or usage procedures

f) Software services vulnerable to cyber attack

g) Software causing operational problems to endpoint devices or University networks

h) Untrusted mobile code, viruses, worms, trojans and spyware.

2.13 In all cases of new software requirements, or extensions to existing licences, departments should first engage IT Services to ensure that the required technical and security evaluations take place prior to procurement.

3. Software Procurement

3.1 University software must be purchased in accordance with the **University's financial regulations** and approved by IT Services to ensure that technical, security, licensing, support and value for money requirements can be considered. There must be an assessment of whether the software incorporates adequate security controls for its intended purpose. It must be investigated and taken into account whether proposed new software or upgrades are known to have outstanding security vulnerabilities or issues. The basis of future support and extended support lifetime of the product should also be established.

4. Software Installations

4.1 Software must only be installed on University computers or networks if there are appropriate licenses and its use is in accordance with its licensing rules. By default, end users are not permitted to install software on University computers. Requests for installations should be placed via the IT Service Desk.

4.2 Where local software installation rights have been granted to individuals in Schools or Departments, the same software installation and usage rules apply. Installations must be notified to IT Services and monitored and controlled appropriately. The list of individuals with local software installation rights will be regularly reviewed by IT Services in conjunction with the relevant Schools or Departments.

4.3 Academic or administrative software applications that require installation on or distribution via the University's servers and networks must not be purchased or acquired without prior technical discussion, evaluation and agreement with IT Services.

5. Browser-based Software

5.1 Paid for subscriptions to browser-based software must go through the same assessment process as all installed software and must be approved before it can be used on a BSU device. Subscriptions must be set up using the softwarelicensemanagement@bathspa.ac.uk email as a billing contact, so it can be

managed by the university. Subscriptions should not be set using an individual's email address and must never be set up using a personal email address. Subscriptions should be set up in such a way that they can be managed and transferred on behalf of the university.

5.2 Free browser-based software must go through the same assessment process as all installed software and must be approved before it can be used on a BSU device. Please be aware that most free browser-based software will use the content produced and that your data and content will most likely be sublicensed to the software owner as soon as you accept their T&Cs. All free software must be risk assessed and the requester must ensure that content and data sharing policies are understood by them and their students.

6. Software Metering

The use of all software installed on the University's networks (including those managed by Schools or Departments) must be controlled and monitored to ensure compliance with licensing agreements and to inform decisions on re-licensing and value for money. IT Services reserves the right to remove and redeploy unused software in order to elicit best value for money from existing licences.

7. Software and Data Security

All applications installed or accessed through University networks or end user devices, including operating systems, firmware, and browser-based software must be supported by a supplier that provides regular fixes for security vulnerabilities. All high-risk or critical security updates for applications, associated plugins, operating systems and firmware must be installed within 14 days. Applications that are no longer supported and no longer receive security fixes must be removed and in the case of hardware equipment, these should be in a planned upgrade plan that meets the supported security updates. Any application that accesses the internet in any way must have Single Sign On (SSO) or Multifactor Authentication (MFA) capabilities to meet Cyber Essentials requirements.

8. Software Audits

IT Services will operate software asset discovery tools in order to audit software installations on the University's networked computers and servers on a regular basis, to compare them against licences owned by the University. Employees with University laptops or computers which are normally located off campus must produce them for software audit at the request of IT Services.

9. Permitted Use of University Software

Unless explicitly authorised, all University software is only for academic or research use, or for the purposes of the University's business and administration, and not for consultancy work or commercial course delivery. Before using University software for consultancy or other external work, users must contact IT Services to check

whether such use is permitted. Similarly, University software must not be used by placement students for the benefit of their employers and does not extend to the use of Partner organisations unless expressly permitted in written confirmation from IT Services.

10. In-house Software Applications

Non-commercialised development of software applications that may require installation on the University's networks or support from IT Services, or which may perform a core administrative or academic function, must not be undertaken without discussion and agreement with the Chief Information Officer or Chief Technical Officer. All such software must follow the guided processes for in-house development.

11. Software Disposal

University software licences must not be given away or sold for use outside the University. All software on University computers that are being disposed of must be securely destroyed.

12. Staff and Student Leavers

Staff who leave the University must return their BSU-issued devices, which provide access to University applications and systems, and must cease using any University provided web-based applications immediately upon leaving employment. Students who leave the University and who have installed University-provided software or stored University data on their personal devices must remove all such software and data immediately and must discontinue any access to University provided web-based applications.

13. Contractors

Contractors, suppliers and temporary staff at the University are covered by the terms of this policy and must not introduce unlicensed or inappropriate software to the University's computers or networks.

Document Details

Responsible Office: IT Services

Responsible Officer: Chief Information Officer

Approving Authority: Vice-Chancellor

Date of Latest Approval: 20 April 2026

Effective Date: 21 April 2026

Related Policies and Procedures: Computer Use Regulations

Supersedes: V1

Next Review Due: April 2029