SOFTWARE USAGE AND CONTROL POLICY

1. Purpose and Scope

The management, accountability and secure configuration of software used within an organisation forms an important element of a sound information security management process. If software is not identified and controlled (using a register), managed correctly (procured, patched, updated), and securely configured, then the University leaves itself open to having unmanaged vulnerabilities and poor processes in place that may lead to compromised data confidentiality, integrity and availability as well as possible reputational damage.

This document forms the University of Reading's *Software Usage and Control Policy* which supports the *Information Security Policy*. Complying with the Policy will help ensure that consistent controls are applied across the University to reduce exposure to security breaches associated with computer software.

1.1 This policy applies to all staff and students involved in the specification, installation, use or maintenance of software used on University of Reading IT resources.

1.2 It comprises all software used whether purchased outright, renewed/leased, hosted via a third party (Software as a Service), freeware or shareware.

1.3 Software includes operating systems (macOS, Windows, etc.), applications (Internet browsers, Outlook, Word, etc.), and IT system tools (auditing tools, anti-virus, intrusion detection systems, etc.).

2. Requirements and Key Principles

2.1 All software shall be configured securely. For example:

- Ensure least privilege of access to services and applications.
- Updates, patches and configuration changes issued by the vendor shall be implemented as soon as practicable.
- Identify the processes that are required from software and disable the remainder.

2.2 Support contracts, where appropriate, should be arranged with the software vendor for through life support.

2.3 No modifications should be made to the software without confirmation that the vendor can continue to provide support.

2.4 Access to operating system, application configurations and IT management tools shall be restricted to authorised personnel only, as per the principle of least privilege.

2.5 Software integrity in live use must be maintained. DTS will carry out manual/automated checks periodically for unauthorised software to help prevent breaches of software integrity.

2.6 A full review of software and licences shall be completed at least annually.

2.7 As per the *IT User Regulations;* Users shall only use software and other resources in compliance with all applicable licences, terms and conditions. Breaches of these regulations by staff will be handled in accordance with the University's Disciplinary Policy.

Software Requests

2.8 Additional software is requested via the IT Service Desk or the University's Software Store (http://softwarestore.reading.ac.uk/).

- All software purchasing requests must be raised via the IT Service Desk and Software Management Tool.
- Software that must require a paid-for licence must go through the University's defined procurement process.

Software Management

2.9 DTS shall maintain a central register of all software they have purchased and/or installed and will maintain a library of corresponding software licences. The DTS Software Register, where possible, shall provide:

- Title and publisher of the software.
- Price.
- Purchase order number.
- Source and date of software acquisition.
- Product version and serial number.
- Renewal date.
- Location of backup copies.
- Team/person responsible for supporting/maintaining the software.
- Location of each installation/assigned user.
- Operating system of machine it is installed on.

2.10 Schools/functions that purchase and/or install software independently shall maintain their own software register or utilise the DTS software register.

2.11 Software audits may be carried out with little or no advance warning so the software register/s must be kept up to date.

Unsupported Software

2.12 Unsupported software is prohibited at the University unless it has been risk assessed and approved for use by the DTS Department. Compensating security controls shall be applied to mitigate the risk of using unsupported software (e.g. isolation, network segregation) provided there is a valid business justification for its use.

2.13 Peer-to-peer (P2P) software is prohibited on any device physically connected to the University network. This includes University and privately owned devices. Users that require P2P software for official University of Reading use, must apply via the IT Service Desk.

Software Removal

2.14 Software found that is not licence compliant must be brought into compliance promptly or be uninstalled.

2.15 Software known to be causing a serious security problem, that cannot be sufficiently mitigated, shall be removed.

2.16 Application software and systems that are no longer required should be decommissioned.

2.17 When decommissioning a computer system, appropriate measures must be taken regarding software and data stored on it. Software must be removed where not doing so potentially leads to breaking licence terms. See the *IT Equipment Disposal Policy* for further information.

Privately Owned Computers

2.18 When students or staff leave the University of Reading, University software entitlements for software installed on personally owned devices cease (in most cases). As such all software must be immediately removed.

3. Related Policies

This policy sits beneath the University of Reading's overarching *Information Security Policy.* This and other supporting policies can be found here:

http://www.reading.ac.uk/internal/imps/policiesdocs/imps-policies.aspx

Document control

VERSION	SECTION	KEEPER	REVIEWED	APPROVING AUTHORITY	APPROVAL DATE	START DATE	NEXT REVIEW
1.0	N/A	DTS	Biennially	University Policy Group	May 20	May 20	May 22