BOND UNIVERSITY	**SOFTWARE AND SOFTWARE SUBSCRIPTIONS POLICY**
Policy Owner	Director, Information Technology Services
Contact Officer	Head, Customer Technology Services
Endorsement Authority	Vice President Operations
Date of Next Review	August 2027

1. PURPOSE AND OBJECTIVES

The purpose of this Policy is to outline the acceptable use of Software utilised by Bond staff and students in undertaking Bond activities, and to protect the University and its Authorised Users from legal action resulting from the use of non-authorised Software, to ensure cyber-security risks are minimised for data protection and information privacy is assured, existing supplier and brand agreements are leveraged, solutions are reliable, serviceable and supported, and to gain efficiencies from centralised software procurement.

Software for the purposes of this Policy includes:

- Software installed on University assets and devices
- Software as a Service
- Cloud based Software Subscriptions
- Free Software
- Software developed by or on behalf of Bond.

2. AUDIENCE AND APPLICATION

This Policy applies to all Authorised users of the University ICT Services managed by the University or third-party providers on behalf of the University, both on and off campus.

3. ROLES AND RESPONSIBILITIES

Role	Responsibility
Authorised Users	▪ Comply with this Policy and associated procedures.
Manager, Customer Support Services	▪ IT Service Desk management ▪ Field initial requests for software
Head, Procurement and Vendor Services	▪ Software procurement assistance
ITS Technical Architecture Group (TAG)	▪ Facilitate the assessment of new software through Bond's Software Approval procedures
Manager, End Device Services	▪ Facilitate installation / access to software via Bond managed devices.
Manager, Microsoft Platforms	▪ Facilitate Enterprise application access through SSO or other controls
Director, ITS	▪ Approve policy changes and exceptions. ▪ Periodically send a reminder of the obligations of this Policy to all Authorised Users.
Faculties and Business Units authorised staff	▪ Ensure Policy is adhered to and that the benefits and cost of new requests are justified.

4. POLICY STATEMENT

4.1 Use of Software

4.1.1 Bond University and all Authorised Users will only use legally acquired software that is configured and used in accordance with the License terms and conditions.

4.1.2 The making of Illegal Software copies or use of such copies is prohibited.

4.1.3 The use of all software on Bond managed devices, including cloud-based Software Subscriptions, must comply with all relevant University policies.

4.1.4 Free Software may only be used if the free Licence conditions explicitly allow for use in an enterprise and has been assessed as part of Bond's Software Approval procedures.

4.1.5 Software purchased by the University is licensed primarily to the University for use on University Computing Facilities, however approval for some software may be granted to Authorised Users for use at home or other locations on non-University owned computers during the course of work or study with the University. This is subject to the contractual obligations and conditions of use as stated in the software license agreement.

4.1.5.1 Any request for use of software on staff personal devices must be approved by ITS and if granted the inclusion of MDM (Intune) software will be installed also. The MDM ensures that any applications and data related to work is secured and can be wiped in the event of a lost or stolen device.

4.1.6 **Authorised Users must:**

- Comply with the contractual obligations and terms and conditions of use stated in the software license agreements entered into by the University.
- Discontinue use and un-install the software from non-University owned devices upon cessation or termination of employment or completion of study, or upon notification by the University of its termination of (or changes to) the software license arrangement.

4.1.7 **Authorised Users must not:**

- Attempt to access software or subscriptions for which authority has not been granted.
- Interfere or attempt to interfere with the operation of any software or the access to that software
- Download, install, delete or modify software on Bond Computing Facilities and devices without authorisation from Information Technology Services
- Process or store Bond data on personal devices or personal subscriptions.

4.2 Software Environments

4.2.1 All Computing Facilities must use the Standard Operating Environment, except where approval has been granted by the Director, Information Technology Services.

4.2.2 Information Technology Services will maintain and publish a catalogue of Authorised Software.

4.2.3 Information Technology Services will make available, software approved as part of the Software Request process. Where possible, software will be made available on a self-service basis via the University Corporate Portals

4.2.4 All computing facilities must run Bond University's chosen anti-virus software. No one should attempt to disable or interfere with the anti-virus software and must report any instances in which they believe the software has been disrupted from normal operation to Information Technology Services.Single Sign-on to be established for any user authentication to software utilised by Bond. If SSO is not available, special consideration must be requested via ITS.

4.3 Software Procurement

4.3.1 Information Technology Services is responsible for the purchasing, renewal, and disposal of all software used in Bond Computing Facilities, unless agreed with the Director, ITS

4.3.2 Authorised users may request the purchase or installation of software via the Software Request Process.

4.3.3 ITS will assess all software requests to ensure chosen solutions are fit for purpose and meet policy and architectural requirements prior to any procurement.

4.3.3.1 If the software complies with the approved ITS exception process, the faculty's responsible officer must ensure compliance with assessment and ROI conditions.

4.3.4 Software which has been personally purchased outside of the Procurement Policy Framework will not to be installed on Bond University owned assets and are not to store or process Bond data.

4.3.5 Software and software subscriptions purchased to include SSO functionality. Any exceptions to be requested via ITS TAG.

5. Software Licence Monitoring

Software Licence monitoring is undertaken by Information Technology Services to ensure that the University maintains compliance in terms of currency, legality, and quantities of Licences as well as to determine unauthorised and/or Illegal Software installed on University ICT Services. For each software application or subscription, both licence compliance and usage reports can be produced as outcomes of this monitoring.

The University strictly adheres to all obligations regarding software licensing and manages the risks accordingly. Under unique circumstances some staff may have administration privileges to install software on university computer assets in the pursuit of teaching, learning and research, these privileges are governed and regulated by the Authorised Software Policy. Furthermore, under the ICT Acceptable Use Policy, the University reserves the right to monitor or review information stored on the Facilities (clause 4.3).

6. DEFINITIONS, TERMS, ACRONYMS

Authorised Software	Software that has been assessed, approved and is being operated under duly acquired Licence terms and conditions and in accord with university aims and objectives.

Authorised Staff Member	Bond University staff who hold executive positions such as Deans, Associate Deans, Vice Presidents, Directors, Faculty Business Directors, Deputy Directors, General Managers and their executive assistants.
Authorised Users	A person who has been provided with an Authentication Credential by the University to access University ICT Services.
Computing Facilities	All computing and telecommunication facilities and services, provided in offices, meeting rooms, laboratories, lecture theatres and teaching spaces, residences and other areas on campus and services provided through local or remote access from off campus.
Free Software	Software offered free of charge usually for private, personal use and not for use in an enterprise or for commercial purposes.
Illegal Software	Software that is copied or used outside the terms of the software License. Such actions are illegal under the Commonwealth Copyright Act and carry high penalties.
License	The right to use the software granted by the licenser to the licensee under the conditions of the agreement.
Mobile Device Management (MDM)	Security software used to secure, monitor, manage, and enforce policies on mobile devices used by employees.
Single Sign-on (SSO)	Authentication process allowing user access to multiple applications or services with one set of login credentials rather than requiring users to remember separate login credentials for each application.
Software as a Service (SaaS)	Cloud hosted corporate software accessed via browsers.
Software Subscription	Cloud based services, generally accessed by a limited number of people and on a monthly basis.
Standard Operating Environment (SOE)	A specification for a standard computer architecture and software applications that is used within the University on Bond Computing Facilities.
University ICT Services	Facilities and/or Services provided to an authorised user (wired or wireless) including software, internet usage, email, communication devices, hardware and computing infrastructure under the control of the University (or a third-party provider on the University's behalf) that provides access to information in online or electronic format.

7. RELATED DOCUMENTS

Procurement Policy (FIN 7.5.1)
ICT Acceptable Use Policy (INF 6.1.11)
Copyright Compliance Policy (TL 3.8.1)
Social Media Policy (INF 6.1.1)
Software Request Process
Software Assessment
Curriculum and Cloud Based Software Process
University Credit Card Procedure
Financial Delegations Policy (FIN 7.1.3)
Data management policy (draft)

8. MODIFICATION HISTORY

Date	Sections	Source	Details
26 August 2024	Whole document	Director ITS	▪ Policy name change ▪ Clarification of software subscriptions. ▪ Clarification of data access restrictions from personal devices. ▪ Roles and responsibilities updated.

			▪ Reference to software request processes and assessments.
24 January 2023	1,2,3, 4.2.5, 4.3.2, 4.3.3, 6, 7	Director ITS	Reference to ITS software procurement procedures and authorised users and authorised staff members.
19 November 2019			
12 May 2009			Date First Approved

APPROVAL AUTHORITY: Vice Chancellor