Richmond
American University
London

SOFTWARE INSTALLATION AND DIGITAL COMMUNICATION POLICY

Introduction

The purpose of this policy is to establish guidelines for the procurement, installation, and use of software applications and digital communications tools and platforms at Richmond American University London (University). This policy aims to ensure the integrity, confidentiality, and availability of University data, prevent security incidents, and protect the University's assets.

The scope of this policy includes:

- All University employees, contractors, students, and anyone who uses University computing resources.
- All software applications and communications platforms used for University business, whether they are installed on University-owned or personal devices.
- All software applications and communications platforms installed on University devices, whether they are used for University or personal purposes.
- For the avoidance of doubt, this policy's scope includes any browser extensions and web-based communications platforms, even if they do not require any software to be installed on the user's device/s.

Policy

1. Software and application procurement

- The University will acquire software and applications from reputable vendors, and only after a thorough evaluation of their features, compatibility, licensing, and security requirements. All procurement will be conducting in accordance with the University's Third Party Policy.
- All software and application purchases must be approved by the University's IT department.

2. Software and application installation

- Only the IT Department may install software and applications on University devices.
- All software and applications must be installed from a trusted source, and the IT Department will verify the authenticity and integrity of the software before installation.
- Users must not modify, tamper with, or delete any software or application files, libraries, or configurations without prior approval from the IT department.

3. Software and application use

- Users must use software and applications only for their intended purposes and in compliance with University policies, procedures, and applicable laws.
- Users must not share software or applications with unauthorised individuals or install them on personal devices without prior approval from the IT department.
- Users must report any software or application-related security incidents or vulnerabilities to the IT department promptly.

4. Software and application updates and patches

- The IT department will manage the installation of software onto University devices, and will manage the deployment of application updates and patches to ensure the security and stability of University computing resources.
- Users are responsible for performing patching and updating of University software deployed to personal devices, and are required to ensure all such software is updated promptly and regularly.
- Users must not delay or refuse to install critical software or application updates or patches.

5. Communications tools

Communication tools are software applications that allow 1 to 1 messaging and file share as well as group-based collaboration. The University provides the following communication tools for use on University owned devices, in accordance with this Policy:

- Microsoft Teams
- Microsoft Outlook (email)

Staff and students may also install Microsoft Teams and Outlook on personal devices, in accordance with the relevant licence agreement, which the IT Department would be happy to clarify if a user is unsure of their entitlement.

In addition, University recognises the use of other communication platforms, many of which are free to use and not covered by University licence agreements. Such platforms include, but are not limited to:

- WhatsApp
- Zoom
- Facebook Messenger
- WeChat
- Telegram
- TikTok

Personal use of any of these platforms, when used on personal devices, falls outside the remit of this policy, and outside the University's control. The IT Department would be happy to offer guidance and best practice advice, to help you keep your personal device and data secure.

However, this policy does restrict the use of these – and other – communications tools, when installed on University devices, as some can create holes in the University's cyber defences and potentially expose University data to cyber threats. As above, under "Software and application installation" the installation of any digital communication tool onto a University computer or device is strictly prohibited, unless performed by a member of the IT Department.

Furthermore, since the level of security and encryption offered by many of these platforms is limited, or non-existent, they are not to be used for personal, privileged or confidential communication. WeChat and TikTok, in particular, are known to be unencrypted and actively monitored by external parties outside the United Kingdom. For the avoidance of doubt, this applies equally to University-owned and privately-owned devices.

It is accepted that since some platforms, including Teams and WhatsApp, do not function in all territories, there may be occasions when users have no option but to use alternative products for University business. This may include users in the UK who are communicating with people overseas. In such cases, the University approves the use of alternative platforms, but care must be taken to ensure no confidential, personal or privileged information is transmitted over potentially insecure channels.

As above, only the IT Department may install software on University devices, so users should consult the IT Department before electing to use such a product.

5.1. Use of other platforms

Given the above, the University accepts that other platforms will be used from time to time, but the following conditions must be observed:

- Gain the permission of individuals who you intend to add to groups, as their details will be shared with all members on that group
- Individuals must never be pressured into using such platforms, and those who choose not to, should not be put at any disadvantage
- Remove individuals from Groups when they are no longer required in them, and/or when employees or students leave the University. This is especially important for Group Admins
- Limit the data exchange to what is needed and appropriate, avoid adding any sensitive data on students or staff/faculty
- Avoid sharing documents and images
- Avoid discussing personal or sensitive matters on organisational groups
- Do not share inappropriate material or content which could cause offense
- Maintain a strong security posture on your device, this should include updating the device when prompted and locking the device with pin, password or biometric

6. Non-compliance

Any misconduct or breach relating to this policy by a University employee may lead to disciplinary action under the appropriate procedures laid out in the Employee Handbook.

Policy violations by students will be dealt under the Student Code of Conduct.

7. Exceptions

Any exceptions to this policy must be approved by the Head of Information Technology.

VERSION MANAGEMENT

Responsible Department: Information Technology			
Approving Body: Operations Committee			
Version no.	**Key Changes**	**Date of Approval**	**Date of Effect**
1.0	Initial Version	17/05/2024	September 2024
		Restricted Access? *Tick as appropriate*: Yes ☐ No☒	