Richmond
American University
London

SOFTWARE APPLICATION AND DIGITAL COMMUNICATION POLICY

Introduction

1. The purpose of this policy is to establish guidelines for the 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.

2. The scope of this policy includes:

    2.1 All University employees, contractors, students, and anyone who uses University computing resources.

    2.2 All software applications and communications platforms used for University business, whether they are installed on University-owned or personal devices.

    2.3 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.

Software And Application Use

3. Users must use software and applications only for their intended purposes and in compliance with University policies, procedures, and applicable laws.

4. Users must not share software or applications with unauthorised individuals or install them on personal devices without prior approval from the IT department.

5. Users must report any software or application-related security incidents or vulnerabilities to the IT department promptly.

Software And Application Updates And Patches

6. 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.

7. 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.

8. Users must not delay or refuse to install critical software or application updates or patches.

Communications Tools

9. 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:

    9.1 Microsoft Teams

    9.2 Microsoft Outlook (email)

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

11. 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:

    11.1 WhatsApp
    11.2 Zoom
    11.3 FaceBook Messenger
    11.4 WeChat
    11.5 Telegram
    11.6 TikTok

12. 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 w may offer guidance and best practice advice, to help you keep personal device and data secure. **Faculty and staff are strongly advised not to use social media to contact and communicate with students.**

13. 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. 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. 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.

14. As 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.

15. 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.

16. Exceptions to this may only be granted following a written request to the IT Head, supported by a clear business case and agreement by a senior line manager (Director level or 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.

Use Of Other Platforms

17. Where the use of other platforms has been approved the following conditions must be observed:

    17.1 Gain the written permission of individuals who you intend to add to groups, as their details will be shared with all members on that group.

    17.2 Individuals must never be pressured into using such platforms, and those who choose not to, should not be put at any disadvantage.

    17.3 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.

    17.4 Limit the data exchange to what is needed and appropriate, avoid adding any personal or sensitive data on students or staff/faculty.

    17.5 Avoid sharing documents and images.

    17.6 Avoid discussing personal or sensitive matters on organisational groups.

    17.7 Do not share inappropriate material or content likely to cause offense.

    17.8 Maintain a strong security posture on your device, this should include updating the device when prompted and locking the device with pin, password or biometrics.

Non-Compliance

18. 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.

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

Exceptions

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

VERSION MANAGEMENT

Responsible Department: IT			
Approving Body: University Board (on recommendation of Operations Committee)			
Version no.	**Key Changes**	**Date of Approval**	**Date of Effect**
1.0	Initial Version	24 July 2025	September 2025
		Restricted Access? ***Tick as appropriate*: Yes ☐ No X**	