Richmond
American University
London

BRING YOUR OWN DEVICE POLICY

Purpose

1. The purpose of this policy is to establish guidelines for the use of personally owned digital devices (computers, smartphones, tablets, etc) if connected to the University's network and/or used to process University data. This policy aims to ensure the continued operation and stability of the University's IT estate, protect the integrity, confidentiality, and availability of University data, prevent security incidents and protect the University's assets.

Scope

2. The scope of this policy includes:

    2.1 All University employees, contractors, students, visitors, and anyone who processes University data (known as Users).

    2.2 Any digital device not owned or managed by the University, which is connected to the University's network, for whatever purpose.

    2.3 Any digital device not owned or managed by the University, which is used to access or process University data, regardless of where it is located.

Introduction

3. Using a personal device as an authentication tool, as part of a multi-factor authentication system, does not process any University data, and is therefore not governed by this policy, unless the device needs to connect to the University network for it to operate.

4. The University provides computers to all permanent staff. However, adjunct, part-time, visiting and contracted staff may be required to use their own devices, even while on campus. It is also accepted that some staff may prefer to use a personally-owned computer, rather than their University laptop, when working remotely.

5. Students are expected to possess their own computers to use for their studies. While a small number of shared computers are available for student use, the expectation is that students will generally use their own laptops, both on campus and while studying off-site.

6. The University permits staff to add their University credentials to personal devices, in addition to their University laptop (for example, a smartphone.) Such devices may be used remotely or connected to the University network while on-campus.

Policy

Connecting Personal Devices to the University Campus Network

7. The University campus has fast WiFi connectivity throughout, and it is permitted to connect personal devices to this. Personal devices will automatically be associated with the BYOD network, which gives access to the internet only, isolating unmanaged devices from the University's internal domain and restricted data.

8. The University campus also has a wired network for connecting University desktop computers, printers and servers. For cyber security and data privacy reasons, it is strictly prohibited for anyone to connect a personal device to the wired network.

9. Personal devices that do not have wireless capabilities will not be able to connect to the University's network.

Using Personal Devices to Access University Data or Systems

10. For cyber security reasons, personal devices are prevented from accessing internal systems (for example the University's file servers, Finance system, etc.) Personal devices can only access data or systems which are published to the internet, including Microsoft SharePoint and other cloud-based services, for example, BlackBoard.

11. The University offers a VPN (Virtual Private Network) facility for staff working remotely using their University-managed computers. This facility is not available to students or for personally-owned computers.

12. If staff require access to internal systems (for example University file servers) from a personal device, the University operates a Remote Desktop server for this purpose, and the IT Department will be able to offer guidance on its use.
    The Remote Desktop server is not available to students.

13. Users must keep University data secure, and should not permit anyone else, including family members, to have access to their data, emails or systems. Devices which have been configured to access University systems should not be shared.

14. Devices which access University data should be locked with a password or PIN code when not in use and should never be left unattended in public places.

15. Data should be stored and edited online, if available, and the downloading of data locally should be avoided whenever possible. Where data is downloaded locally this should only be stored as long as is necessary and should be deleted when no longer required.

Device Requirements

16. Users are responsible for selecting, purchasing and maintaining their device/s. If requested, the IT Department can offer guidance on device selection, but are not obliged to offer technical support on issues with personal devices.

17. The operating system installed on any device connecting to the University network and/or processing University data must be unmodified, regularly patched and updated and have an appropriate up-to-date antivirus solution.

18. Connecting to the University's Microsoft 365 environment (including email access) enforces certain minimum levels of security (for example the existence of a PIN code or password) and enables the IT Department to forcibly wipe all data from a device if it is lost or stolen.

Compliance

19. The IT Department has the right to audit/inspect any device that connects to the University network, if it is suspected to be posing a cyber security risk, or in breach of this or other University policies. Any device found to be posing a risk will be forcibly removed from the network until the issue can be resolved.

20. Loss of a device containing University data constitutes a potential data breach, and must be reported immediately to the Data Protection Officer at dpo@richmond.ac.uk

21. 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.

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

Exceptions

23. Any exceptions to this policy must be approved by the Head of Information Technology. Student appeals will be heard through the complaints and appeals process.

VERSION MANAGEMENT

<table>
<tr><td colspan="4"><b>Responsible Department: IT</b></td></tr>
<tr><td colspan="4"><b>Approving Body: University Board (on recommendation of Operations Committee)</b></td></tr>
<tr><td><b>Version no.</b></td><td><b>Key Changes</b></td><td><b>Date of Approval</b></td><td><b>Date of Effect</b></td></tr>
<tr><td>1.0</td><td>Initial Version</td><td>24 July 2025</td><td>September 2025</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2"><b>Restricted Access?</b>
<b><i>Tick as appropriate</i>: Yes ☐ No X</b></td></tr>
</table>