Bring Your Own Device (BYOD) Policy

Policy Category:	General
Subject:	Use of personal, unmanaged devices to connect to University systems and access organisational data
Approving Authority:	University Executive
Responsible Officer:	Senior Vice-President (Operations)
Responsible Office:	IT
Related University Procedures:	Password Procedure Email and Collaboration Tools Procedures Mobile Device Procedure Information Security Procedures Data Protection Procedure Code of Connection Procedure
Related University Policies:	IT Acceptable Use Policy Research Data Management Policy Identity Management Policy Records Management Policy Data Protection Policy Mobile Device Policy
Effective Date:	February 2024
Supersedes:	First issue
Last Review:	N/A
Next Review:	February 2025

1. PURPOSE & SCOPE

1.1 The University recognises the benefits that can be achieved by allowing staff to use their own devices whilst working, whether this is at home, on campus or whilst travelling, and the purpose of this policy is about reducing the risk when using such personal devices. Risks include devices being lost or stolen, being used by others who are not authorised to access University information or being exploited in such a way as to put University data at risk.

1.2 This policy applies to any internet connected device not centrally managed or supported, which is used to access University systems and data, or to store, process or transmit University information.

1.3 Information classified as restricted or highly restricted (or corresponding classification) should only be accessed using University-supported devices that are connected to trusted networks as laid out in the IT Acceptable Use Policy, sections 3.1, 3.2, 3.3, and 4.3.

1.4 If you are in any doubt whether your personal device meets the security requirements of this policy, please raise a service request via the IT Service Desk to IT Assurance.

2 ROLES & RESPONSIBILITIES

2.1 All users of personal devices accessing University information, applications, and/or systems shall comply with this policy and any related policies and procedures. It is the user's responsibility to consult the device's operating instructions and understand how to correctly apply all settings, software and controls as laid out in this policy.

2.2 Heads of departments/faculties and their deputies shall ensure that all members of their department/faculty are aware of this policy.

2.3 Data custodians are responsible for knowing where data is held and that it is safe.

3 PERSONAL DEVICE SECURITY

3.1 The following security requirements must be present on personal devices before any attempt to access KCL organisational data is made:

- Personal devices must use a supported operating system which has up to date security patches and fixes applied. Wherever possible, 'auto-updates' by the vendor should be enabled.
- To prevent unauthorised access, devices must use appropriate authentication settings, for example enabling a security PIN, passcode, or biometric access control. If a device has a weak or default credential which allows access to it, this must be changed before accessing any KCL organisational data.
- Personal devices used to access or process KCL organisational data must be protected by anti-malware software where applicable.
- Laptop and desktop computers must have a software firewall installed and enabled. Windows and Apple Mac computers will have this functionality built in.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing KCL organisational data.
- Personal devices need to adhere to conditional access policies when used to access KCL organisational data. Further details and up to date information on this may be found in the BYOD procedure.

4 USE & MAINTENANCE

4.1 Users shall take great care when accessing University data in public places, as information may be viewed by unauthorised individuals by way of eavesdropping or shoulder surfing.

4.2 Users shall keep their operating systems and applications up to date with security updates.

4.3 Users shall only use a device if it is receiving operating system updates from a recognised vendor. A device should not be used once the vendor ceases to provide security updates.

4.4 Users must set up a separate user account profile without Administrative or Elevated privileges on their device for the purposes of accessing University data on devices which support multiple user accounts.

4.5 The University reserves the right to restrict access for devices deemed to be detrimental to the security or operation of its systems.

5 DATA GOVERNANCE

5.1 Users shall only process information on a device in accordance with the IT Acceptable Use policy.

5.2 Users shall not use a personal device as the sole repository for University information. Users must ensure that any data exported from University systems is handled in such a way as to maintain the confidentiality and security of that data.

5.3 Users shall ensure that all KCL data, information and software stored on the device is securely deleted:

- At the end of their engagement with the University.
- When they stop using the device and/or before the disposal of the device.

5.4 When selling, transferring, or disposing of a device that has been used to access organisational data, it is essential that all University information assets are removed. Where possible the device should be wiped and/or factory reset.

5.5 Any personally held backups must also be securely deleted. For more guidance see: Erasing devices - NCSC.gov.uk

6 DEVICE LOSS OR UNAUTHORISED ACCESS

6.1 Users shall report loss of, or unauthorised access to, a personal device which has been used to access KCL organisational data using the University's Data Breach procedure without delay and will co-operate in wiping University information from the device wherever possible and reasonable.

6.2 Any misuse, or suspected misuse of a device or breach of this policy will be dealt with in accordance with the IT Acceptable Use policy.

7 DEFINITIONS

- **Data custodians** are individuals who have operational level responsibility for the capture, maintenance, and storage of data.
- **Devices** includes all types of hosts, networking equipment, servers, networks, and end user devices such as desktop computers, laptop computers, thin clients, tablets and smartphones; whether physical or virtual.
- **'Jailbreaking'** is the process of exploiting the flaws of a locked-down electronic device to install software other than what the manufacturer has made available for that device. Jailbreaking allows the device owner to gain full access to the root of the operating system and access all the features.
- **Licensed and supported software** is software that you have a legal right to use and that a vendor has committed to support by providing regular updates or patches. The vendor must provide the future date when they will stop providing updates. (Note that the vendor

doesn't need to have created the software originally, but they must be able to now modify the original software to create updates).

- **Malware** is software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system.
- **Organisational data** includes any electronic data belonging to your organisation, for example, emails, calendars, documents, database data, financial data etc.
- **Organisational service** includes any software applications, cloud applications, cloud services, user interactive desktops and mobile device management (MDM) solutions that your organisation owns or subscribes to. For example: web applications, Microsoft 365, Google Workspace, mobile device management containers, Citrix Desktop, Virtual Desktop solutions or IP telephony.
- A **personal device** is piece of equipment which can be connected to the internet which is personally owned and personally enabled, but accesses organisational data.
- **Servers** are devices that provide organisational data or services to other devices as part of your organisation's business.
- **Shoulder surfing** is the practice of spying on the user of a cash-dispensing machine or other electronic device to obtain their personal identification number, password, etc.
- **Software** includes operating systems, commercial off-the-shelf applications, plugins, interpreters, scripts, libraries, network software and firewall and router firmware.
- **Standard Operating Environment (SOE)** refers to a given computer operating system (OS) and its associated hardware and software applications, used by an organisation to cost-effectively and efficiently deploy these with custom configurations as required. SOEs also serve to expedite software updates and service packs (major updates to OSs).
- **The National Cyber Security Centre** is a UK-based organisation that provides advice and support for the private and public sector in how to avoid computer security threats.
- The University's **Code of Connection (CoCo)** clearly defines the base levels of security 'hygiene' and technical controls that must be in place to access the computer network and/or services at King's College London.
- **University system** is defined as any University system or application which supports the University's academic and business processes, e.g. SITS, finance system, HR system, KEATS.

8 DOCUMENT CONTROL

8.1 This policy shall be reviewed at least annually, or where a significant change is made.

Version	Date	Name	Role	Changes
1.0	09/02/24	Kate Palmer	Head of IT Assurance	First publication