# Bring Your Own Device Procedure

| | |
|---|---|
| **Effective Date**: | November 2021 |
| **Supersedes**: | New |
| **Next Review**: | November 2024 |

## 1. Purpose and Scope

1.1 The purpose of this procedure is to facilitate secure and lawful access to university information assets in ways that reduce exposure to information security related risks. Individuals are responsible for the success of this procedure.

1.2 This procedure applies to any internet connected device, that is not university supported, which is used to access university systems or to store, process or transmit university information.

1.3 The scope of this procedure covers access to internet based applications using non-university supported devices in the following circumstances:

- Where the data is classed as their own personal data
- Where the information is classified (as per the university's information classification procedure) as external or internal information.

1.4 Information classified as restricted or highly restricted should only be accessed using university supported devices connected to trusted networks as laid out in IT AUP section 3.1, 3.2, 3.3 and 4.3.

1.5 The Cyber Essentials scoped Windows Virtual Desktop (WVD) environment will only be accessible from a standard operating environment device and requires the user to sign a forfeit agreement to confirm they will not use any personally enabled device to access any organisational data. Organisational data includes any solutions and applications provided by KCL.

1.6 If you are in any doubt or wish to raise a query about the scope of this procedure, please raise a service request via the IT Service Desk to IT Assurance.

1.7 This procedure does not apply to information that the university has placed in the public domain.

1.8 The university is not under any obligation to assist users in the connection of a personal device to university systems or networks.

## 2. Procedure

The level of risk should drive any decision about whether it is acceptable to use a personal device to access information on university systems. The following procedural statements should be interpreted with this in mind.

## 2.1 Roles and responsibilities:

2.1.1 All users of personal devices accessing university information/applications/systems shall comply with this procedure and any related policy and procedure. 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 procedure.

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

2.1.3 Student Services shall formally ensure that students are made aware of this procedure.

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

## 2.2 Personal Device Security

2.2.1 Users shall use best efforts to physically secure the device against loss, theft or use by persons who are not authorised to access the device.

2.2.2 Users shall ensure that the device is protected against unauthorised access by security methods that are proportionate to the sensitivity of information stored on, or accessed by, the device. (For example, passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device (see Password procedure for more information about password best practice).

2.2.3 Users shall install appropriate anti-malware software if it is available for the device.

2.2.4 Users shall set the device to automatically lock when the device is inactive or unattended.

2.2.5 Users shall enable remote wipe of at least all university data on the device if this feature is supported.

2.2.6 Users obtaining a second-hand device shall ensure it is reset to its factory settings prior to the first access of university data. This is primarily to avoid exposure to malware.

2.2.7 Users shall not store university information in a way that can be accessed by any other user of the personal device.

2.2.8 Users shall ensure that the device's security settings are configured according to the National Cyber Security Centre's recommended guidelines: Cyber Aware - NCSC.GOV.UK

2.2.9 Users shall ensure that the device is running a supported operating system.

2.2.10 Users shall ensure that the device has not been 'jailbroken' or allow root access to system files.

## 2.3 Use and Maintenance

2.3.1 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.

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

2.3.3 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.

2.3.4 The university reserves the right to block any device deemed to be detrimental to the security or operation of its systems.

### 2.4 Data Governance

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

2.4.2 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.

2.4.3 Users shall ensure that all university data, information and software stored on the device is securely deleted;

a. at the end of their agreement with the university

b. when they stop using the device and/or before the disposal of the device.

2.4.4 Any personally held backups must also be securely deleted. For more guidance see: Erasing devices - NCSC.GOV.UK.

### 2.5 Actions on discovering device loss or unauthorised access

2.5.1 Users shall report loss of, or unauthorised access to, the device using the university's Data Breach procedure without delay and will cooperate in wiping university information from the device.

2.5.2 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, section 15.

## 3. Related policies and procedures

IT Acceptable Use policy and procedure

Data Protection policy

Data Governance policy

Data Breach Management procedure

Records Management policy

Research Data Management policy

Code of Connection

## 4. Definitions

A **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.

A **device** is a piece of portable electronic equipment that can connect to the internet, especially a smartphone or tablet computer.

A **web-based application** is any program that is accessed over a network connection using HTTP, rather than existing within a device's memory. Web-based applications often run inside a web browser. However, web-based applications also may be client-based, where a small part of the program is downloaded to a user's desktop, but processing is done over the internet on an external server.

**Standard Operating Environment (SOE)** refers to a given computer operating system (OS) and its associated hardware and software applications, used by an organization 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).

**Cyber Essentials** is a Government-backed and industry-supported scheme that helps businesses protect themselves against the growing threat of cyber attacks and provides a clear statement of the basic controls organisations should have in place to protect themselves.

**Data custodians** are individuals who have operational level responsibility for the capture, maintenance, and storage of data.

**Malware** is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

**'Jailbroken'** 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.

**Shoulder surfing** is the practice of spying on the user of a cash-dispensing machine or other electronic device in order to obtain their personal identification number, password, etc.

**Virtual LANs (VLANs)** are a solution to allow an organisation to separate users into individual network segments for security and other reasons.

**Eduroam** (education roaming) is the secure, world-wide roaming access service developed for the international research and education community. Eduroam allows students, researchers and staff from participating institutions to obtain Internet connectivity across campus and when visiting other participating institutions

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.

The **National Cyber Security Centre** was launched in October 2016. Its headquarters are in London. It brings together expertise from CESG (the information assurance arm of GCHQ), the Centre for Cyber Assessment, CERT-UK, and the Centre for Protection of National Infrastructure. Specifically the NCSC:

- understands cyber security, and distils this knowledge into practical guidance that they make available to all
- responds to cyber security incidents to reduce the harm they cause to organisations and the wider UK

- uses industry and academic expertise to nurture the UK's cyber security capability
- reduces risks to the UK by securing public and private sector networks.

**Appendix A-Change log**

| Version | Date | Name | Role | Changes made |
|---|---|---|---|---|
| V2.1 | 11/03/2022 | Kirsty Lynch | Senior IT Assurance Officer | Dead links fixed in the related policy and procedure section. |
| V2.2 | 21/04/2023 | Lauren Middlemist | IT Assurance Apprentice | Change control log added as Appendix A |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |