LONDON’S GLOBAL UNIVERSITY

UCL Bring Your Own Device Policy

University College London

Document Summary

Status	Approved
Information Classification	Public
Document Version	Approved by the Information Risk Governance Committee 29-Nov-2021

University College London, Gower Street, London WC1E 6BT
Tel: +44 (0)20 7679 2000
www.ucl.ac.uk

1 Introduction

UCL understands the importance of mobile working and the benefits that can be realised by its users with authorized access to UCL systems and information. However, the use of a personal device for legitimate UCL purposes poses risks. These risks include:

- Disclosure of confidential information if a device should be stolen or lost, or if a device is out of date with security updates, or is compromised (“hacked”).
- Permanent loss of information should a device holding the only copy be lost or stolen.
- Damage to, or corruption of, information
- Failure to comply with legal or contractual obligations.
- Undermining the security of our IT resources and communications systems.

Such risks could result in damage to our information, our systems, our business and our reputation.

UCL intends to allow access to its information by its users, but also must meet its legal, contractual and duty of care obligations.

2 About this Policy

The purpose of this policy is to facilitate secure and lawful access to University information assets in ways that reduce UCL’s exposure to the above risks. Individuals are responsible for the success of this policy.

If you have any questions regarding this policy or have questions about using a personal device for business purposes which are not addressed in this policy, please contact ISG (Information Security Group).

3 Scope

This policy applies to any electronic device that is owned by users which is used to access UCL systems or to store, process or transmit UCL information.

This policy does not apply to information that UCL has placed in the public domain.

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

4 Accountable Roles

All users of personal devices accessing UCL information or facilities shall comply with this policy.

Heads of Departments/Divisions and their deputies shall ensure that all members of their department/division are aware of this policy.

The Registrar and Head of Student & Registry Services shall formally ensure that students are made aware of this policy.

5 Policy statements

The fundamental requirement is that UCL information and systems are protected from unauthorised access. The level of risk should drive what is acceptable for using a personal device to access information on UCL systems.

The following policy statements should be interpreted in this light.

5.1 Personal Device Security

PS1 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.

PS2 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 in accordance with the UCL Information Management Policy.

PS3 Users shall install appropriate anti-malware software if it is available for the device.

PS4 Users shall set the device to automatically lock when the device is inactive or unattended.

PS5 Users shall enable remote wipe of at least all UCL data on the device if this feature is supported.

PS6 Users obtaining a second-hand device shall ensure it is reset to its factory settings prior to the first access of UCL data. This is primarily to avoid exposure to malware.

PS7 Users shall not store UCL information in a way that can be accessed by any other user of the personal device

PS8 Users shall ensure that the device's security settings are configured according to UCL's recommended guidelines, including encryption of the storage.

5.2 Use and Maintenance

PS9 Users shall take great care when accessing UCL data in public places, as information may be viewed by unauthorised individuals by way of eavesdropping or shoulder-surfing.

PS10 Users shall keep their operating systems and applications up-to-date with security updates.

PS11 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.

PS12 UCL reserves the right to block any device deemed to be detrimental to the security or operation of UCL systems.

5.3 Data Governance

PS13 Users shall only process information on a device in accordance with the Information Management Policy and the Information Security Policy.

PS14 Users shall not use a personal device as the sole repository for UCL information. The master copy of any UCL data shall be on a UCL server which has a suitable backup regime.

PS15 Users shall ensure that all UCL data, information and software stored on the device is securely deleted;

a. at the end of their engagement with UCL.
b. when they stop using the device and/or before the disposal of the device.

Any personally held backups must also be securely deleted.

5.4 Actions on discovering device loss or unauthorised access

PS16 Users shall report loss of, or unauthorised access to, the device to the Information Security Group (ISG) without delay and will cooperate in wiping UCL information from the device.

PS17 Any misuse, or suspected misuse, of a device or breach of this policy should be reported to ISG.

The actions in PS16 and PS17 are necessary as UCL is required by law to report data breaches to the Information Commissioner within 72 hours of discovery.

6 Dependencies

6.1 Documents which rely upon this policy:

None at present

6.2 Documents which this policy relies on:

- UCL Information Security Policy
- UCL Computing Regulations (Acceptable Use Policy)
- UCL Data Protection Policy
- UCL Monitoring Computer and Network Use Policy
- UCL Password Policy and Principles
- UCL Policy on Connecting Equipment to the UCL network
- UCL Information Management Policy

7 Related requirements

None

8 Stakeholders

The following roles, or their nominated representatives, should be involved in the review of this document

- Policy Owner
- Chief Information Security Officer
- Director – IT Service Delivery
- Data Protection Officer
- Chair of Security Working Group

9 Policy owner

This policy is owned by the UCL SIRO.

10 Policy contact

Chief Information Security Officer

11 Review plan

This document will be reviewed every year, or more frequently if required, e.g. following changes to related requirements, or to related documents.

12 Sanctions

This policy does not form part of a formal contract of employment with UCL, but it is a condition of employment that employees will abide by the regulations and policies made by UCL.

13 Definitions

See Glossary. ***https://www.ucl.ac.uk/informationsecurity/policy/public-policy/Glossary***

Users: Persons including UCL staff members, contractors, students, and others authorized to access UCL systems and information.

14 Approvals

Endorsed by the Security Working Group	**25-May-2018**
Endorsed by the Information Risk Management Group	**27-Mar-2019**
Approved by the Information Risk Governance Group	**10-Apr-2019**
Approved by the Information Risk Governance Committee	**29-Nov-2021**