Mobile Device Policy

Policy Category:	General
Subject:	Use of mobile devices for accessing and storing KCL data
Approving Authority:	SMT
Responsible Officer:	Senior Vice-President (Operations)
Responsible Office:	IT
Related Procedures:	Password Procedure Email and Collaboration Tools Procedures Information Security Procedures Bring Your Own Device (BYOD) Procedure Data Breach Management Procedure.
Related College Policies:	IT Acceptable Use Policy (ITAUP) Identity Management Policy Data Management Policy Corporate Records Management Policy Data Protection Policy Patch Management Policy
Effective Date:	22/09/2022
Supersedes:	N/A
Next Review:	22/09/2025

I. PURPOSE AND SCOPE

1.1 The purpose of this policy is to clarify:

- The definition of a mobile device
- How mobile devices are registered
- Physical protection requirements
- Restrictions imposed regarding software installation
- Software version and patch management expectations; and
- Restrictions of connection to defined information services.

1.2 This policy applies to all staff, students, researchers, academics, volunteers and contractors at the university using a KCL purchased managed mobile device that fits the definition within this policy, and as such, must be familiar with this alongside the Information Security Policy and Acceptable Use Policy (ITAUP).

1.3 Personal mobile devices and unmanaged KCL purchased devices are outside of the scope of this policy.

II. DEFINITIONS

2.1 Table of definitions

Mobile Device	A portable computing device that: • has a small form factor such that it can easily be carried by a single individual • is designed to operate without a physical connection (e.g., wirelessly transmit or receive information) • possesses local, non-removable data storage and is powered-on for extended periods of time with a self-contained power source. Has a display screen with touch input and/or a QWERTY or accessible alternative keyboard, and may provide users with telephony capabilities. Built-in features for synchronising local data with remote locations. Examples include laptops, smart phones, smart watches, tablets, and ereaders.
Personal Mobile Device	A personal mobile device is broadly defined as any laptop computer, smartphone, tablet, etc. that is purchased and maintained by an individual, not owned by KCL, and is used for personal and business purposes.
Unmanaged KCL Mobile Device	Devices purchased by KCL through departmental, research or other funding directly linked to the College, that are not able to be managed through central processes. Used for business purposes.
Device Registration	Inclusion within an asset register to identify the hardware and device owner information at a minimum.
Data User	Any individual or system that uses data for undertaking university business.
Information	What is conveyed or represented by a particular arrangement or sequence of things, such as data.
IT System	A place or platform where university data can be entered, stored, retrieved.
SOE	Standard operating environment, managed laptops

III. Policy

3.1 ***Principles of mobile device management***

The principles below are in accordance with ISO 27001:2013 and have been adopted by the university to secure institutional data processed by data users on managed mobile devices.

Mobile Device Registration	Laptops provided by IT are logged to the IT asset register and are then distributed to the relevant individuals/ departments.
	All other mobile devices are assets local to the relevant department and should be logged with the relevant internal procedures in that department. Each department is responsible for keeping updated records of all mobile devices including the named device holder and serial number of each device.
Physical Protection requirements	Departments and individuals are expected to conform with standard data security requirements and use any security measures provided by KCL. Devices should not be left unattended at any time unless they are placed in a secure locked location. Devices must have either a password, PIN, pattern, fingerprint or biometric protection enabled. Due diligence for security should also be taken at home and it is not permitted to leave devices unattended in vehicles, outbuildings or other such locations. Devices should not be accessed by any other individuals other than the named device holder.
Software Installation restrictions	Installing any software comes with elements of risk. It is expected that users of mobile devices exercise caution when choosing which applications to install on devices that are used for accessing corporate data. Users of SOE devices will be able to install software from the Software Centre that have been through a testing process. Any other required applications not available on the Software Centre can be requested via the Service Desk.
Software Version and Patch Management Expectations	Departmental mobile devices are not managed by King's IT. It is the responsibility of departments and device holders to ensure that departmental assets are updated with relevant patches as soon as they are made available. All patches should be done in accordance with the Patch Management Policy.

Restrictions of connection to identified services	Access permissions based on least privilege will be applied to user accounts to restrict the connections for authorised users. When connecting to applications and data sources that may contain sensitive, confidential or similar information users should be cautious about how the connection is made. If there is any doubt about the security of the connection users should seek guidance from the Service Desk.

3.2 ***Law, regulations, and standards***

Nothing in this policy precludes any steps that need to be taken to comply with the law to disclose information to external organisations or governmental agencies. The university will work to best practice standards aligning with ISO 27001:2013

3.3 ***Ownership and management of mobile devices***

Managed mobile devices are owned by the university, not by any individuals. A department may have delegated responsibility for some mobile devices. Assigned asset owners have ultimate responsibility to manage the data within their authority in compliance with the law and university policies.

3.4 All users of managed mobile devices have responsibility for preserving the security and integrity of university data. All mobile device users must:

- Treat the data in accordance with the College's information classification procedures;
- Follow IT guidance for remote working;
- Remove any locally stored data that is no longer needed and has been transferred to university storage;
- Request support from IT where needed to adhere to this policy;
- Have proper access controls in place. Any breaches of access controls where personal data is shared inappropriately need to be reported as defined in the data breach management procedure.

IV. Enforcement

4.1 Following the requirements of this policy, other associated policies and procedures will ensure that users comply with the law. However, users should contact the IT Service Desk for advice about any concerns.

Non-compliance with this policy or associated procedures is an infringement of King's regulations and will be investigated in accordance with:

- G27 of the Academic Regulations (students)
- College Ordinances and relevant Human Resources Regulations (academic staff)
- College Capability and disciplinary procedures (for staff other than lecturers, senior lecturers, readers, and professors)

Additionally, the country you are working in may choose to investigate and enforce the imposition of penalties.

The Chief Information Officer (CIO) or designate may remove or limit a user's access to the university's systems or the mobile device on a temporary basis when that is deemed necessary to protect the system or prevent reputational damage to the university, or during an investigation.

On the recommendation of the CIO or designate, further access limitations or permanent denial of access may be imposed by the Senior Vice-President (Operations) or designate.

V. Review

5.1 This policy shall be reviewed at least once every three years.

Appendix A-Change log

Version	Date	Name	Role	Changes made
V1.2	24/04/23	Lauren Middlemist	IT Assurance Apprentice	Change control log added as Appendix A.