Kingston University

Acceptable Use Policy – Mobile & Bring Your Own Devices

Owner name: **Job title:** **Dept/faculty:**	Nigel Smith Head of Infrastructure & Operations Information & Technology Services		
Review Due:	Annual		
Key Policy Legislation	Data Protection Act 1998 Copyright Designs & Patents Act 1988 Computer Misuse Act 1990 Freedom of Information Act 2000 Regulation of Investigatory Powers Act 2000 Electronic Communications Act 2000 Counter Terrorism & Security Act 2015, including related Government and HEFCE Guidance Digital Economy Act 2010 Human Rights Act 1998		
Approval Body Sign Off	Name: UIC	Date	22/4/2016

Version Control			
Version	Date	Author	Change Description
0.1	8/3/2016	Mark Sharma-Drake	Initial Review Draft
1.0	21/4/2016	Mark Sharma-Drake	Final Approved

Contents

1 Equality Statement

Because we value diversity and equality highly we have designed this policy to be fair and inclusive. In putting this policy into practice we expect all members of the University community to abide by the spirit and detail of the Equality Act 2010 and One Kingston, our policy and strategy for equality, diversity and inclusion

2 Policy Title

Acceptable Use Policy – Mobile & Bring Your Own Devices

3 Policy Statement

The University supports staff and students in new ways of working, teaching and learning, and is keen to enable individuals to work from locations that suit them. Increasingly this means supporting the use of mobile devices to access IT services. It is also increasingly common for such devices to be the property of the individual and not managed by the University.

This policy provides guidance on the use of mobile devices in order to protect both the University's information assets and the individual's privacy.

4 Policy Scope

This policy applies to all users of mobile devices, whether University owned or the property of individuals. Typically, such devices will connect to the University network in one of the following ways:

- Connecting KU Wi-Fi.
- Eduroam Wi-Fi.
- Guest Wi-Fi (The Cloud).
- Wired.

Examples of mobile devices include, but are not limited to;

- Mobile/Smart Phones.
- PDAs (tablets).
- Laptops.
- Gaming Consoles.

5 Governance & Review

The policy owner will review the policy content annually at least.

The policy owner will review the policy immediately in circumstance where any detail within the policy has significantly changed.

This policy will be signed in the first instance by the policy owner, with subsequent approval by the CIO and final signoff by the University Information Committee.

All University policy documents must be signed and submitted to the University Secretary's office for record.

6 Related Resources

Acceptable Use Policy – IT Facilities

Acceptable Use Policy – Social Media

Acceptable Use Policy – Email

7 Policy:

7.1 Types of Mobile Device

The University provides mobile devices for staff whose roles require it. A list of standard devices provided by the University is available from I&TS. However, it is recognised that staff, students and visitors also have a need to connect to the University's IT resources using their own devices, which the University has no control over.

The University reserves the right to deny network connectivity access to devices that do not meet minimum security standards, or are found to contain viruses or other malware. We strongly recommend that mobile devices are regularly updated with the latest anti-virus updates, and that mobile phone operating systems are kept current as new releases are made available.

7.2 Personal Use of KU Mobile Devices

It is accepted that University provided mobile devices will be used for limited personal reasons. However, personal use of these devices must comply with the following conditions:

- Excessive charges incurred by personal use should be declared to management and may be charged for.
- Personal use must not be for personal or non-KU financial gain.
- Personal use must adhere to all other KU Acceptable Use Policies.

7.3 Physical Security

Mobile devices should be secured with a suitable user ID, password, PIN or other method of individual authentication.

For staff working in office environments it is strongly recommended that a cable lock be used to secure (mainly) laptops to desks. These are available from I&TS and can be obtained through the Service Desk.

If you must leave mobile devices in vehicles make sure they are locked away out of sight.

Do not leave a mobile device in open view unlocked.

If left overnight in a room accessible to others make sure it is locked away.

7.4 Data Security

Data stored on mobile devices is at particular risk of unauthorised access. In addition to the physical measures listed above, it is important to ensure that the information stored on your mobile device is secure.

University owned laptops supplied since summer 2015 use a data encryption tool requiring a PIN upon power-on. Nobody can gain access to the data stored on the laptop without entering a valid PIN. It is strongly recommended that encryption tools are used on personal devices as well.

Do not store personal, financial or sensitive information on mobile devices.

When working with University information the recommended method for accessing this information is My Desktop Anywhere. Using this facility enables information to be accessed, viewed, edited and stored directly onto the University network rather than the mobile device, thereby ensuring its security.