Imperial College

Mobile Devices Policy

Doc. Ref.	: Mobile Devices Policy
Version	: 1.0
Status	: Approved
Date	: 28/06/2018
Approved by	: Information Governance Steering Group
Review by	: 28/06/2019

Contents

1. INTRODUCTION

1.1 Purpose

This document sets out Imperial College London's policy concerning the allocation and use of College-owned mobile phones and wireless devices (together termed and referred to as 'mobile devices' for the purposes of this policy) issued to staff. Staff issued with College-owned mobile devices are referred to as 'Users' in this document. Further clarification on any points can be obtained from your Departmental Telecoms Representative.

Users and Departmental Line Managers MUST read the whole of this document.

1.2 Scope

All College-owned mobile devices are in the scope of this policy, including all types of mobile phones and tablet devices. For clarification, this policy does **not** apply to mobile devices not owned by College, even when they are used on College premises. All users of these devices must still abide by College's Information Security Policy when using them on the College network.

1.3 Definitions

Mobile data allowance: Monthly payment for a fixed quantity of cellular data traffic that is paid for whether it is used or not. After the allowance has been used up, further use is charged per megabyte at a much higher rate.

Cellular data: Data transferred over the cellular network (3G or 4G). Data used over Wi-Fi (wireless) network does NOT count as cellular data.

Mobex: A five-digit internal number assigned to the mobiles, which usually is the last five digits of the full mobile telephone number and can be used to dial the mobile phone internally. This short number can be used to dial mobiles from College desktop sets and other College mobiles.

2. POLICY

The College will only issue a mobile device where there is a clear business requirement, dictated by the requirements of the user's role. It is ultimately at the discretion of the Head of Department whether to issue a mobile to a staff member or not.

The eligibility of a user for provision of a mobile device should be evaluated against one or more of the following criteria:

- The User is required to be available outside business hours to assist with critical business functions of the College (e.g. responding to emergency situations or 'on-call' service requirements).
- The User is required to regularly make or receive business calls when away from the office.
- The User is required to spend frequent or prolonged periods away from their desk.

- The User is required to spend frequent periods working alone or where there are other health or safety concerns.
- There is an identifiable and proportionate benefit to the College.

Heads of Departments appoint a Departmental Telecoms Representative to order and issue the appropriate mobile devices for Users. The College determines the most appropriate mobile device models to issue to meet the requirements of the role. Eligibility for a mobile device will be reassessed whenever a User transfers to a different role.

Mobile devices may also be issued to a Department or section, rather than to an individual, where there is a clear and legitimate need, e.g. Maintenance Teams or where there is an on-call rota in place.

The College may choose to replace devices when business need or technological change dictates.

Mobile phones are provided to staff members of the College for business use and as such, the phone's number will be published unless, with the appropriate Director's approval, a request is made via the Departmental Telecoms Representative for it to be withheld.

The mobile devices and all peripheral equipment leads/chargers etc. remain the property of the College and must be returned to the relevant Telecoms Representative if the device is upgraded, withdrawn, or on termination of employment. Spare chargers and protective screens/covers are not provided by College. Devices that have reached the end of their working life must be disposed of legally as they fall under WEEE regulations.

3. MOBILE DEVICE USAGE

Mobile devices issued by the College are to be used primarily for work-related business and communications. Devices which are provided solely for business use are tax exempt under Section 316 ITEPA 2003, as long as any private use is not significant (see EIM21613).

All mobile devices **must be secured** with a password or a PIN.

Use of, or subscription to, premium and/or interactive mobile services using a College device is prohibited. This includes, but is not limited to, the downloading or forwarding of ringtones and streaming of videos and television services. Any costs associated with misuse are the responsibility of the User.

College mobile devices must be used in accordance with all applicable legislation and College policies, specifically the College's Information Security Policy and Data Protection Policy.

When visiting public sites, Users should be aware of, and respect, local policies regarding the use of mobile communications devices. For instance, it may be necessary to switch such devices off in Hospitals, Courts etc. If in doubt, local staff will be able to advise on local policies.

If you are using a mobile phone be mindful of being overheard and take steps to protect confidentiality. This can be challenging, particularly on public transport, so the call may best be taken later.

Voicemail has been provided on **all** College handsets so that messages can be left if you are unable to answer a call. Voicemail greetings should be personalised by the user with a suitable message which invites the caller to leave a message.

If you are using a data-centric device such as a smartphone or a tablet it is recommended that you connect to Wi-Fi services where available ensuring your mobile data allowance can be used where no Wi-Fi is available.

Please note: using cellular data without a data package is charged per MB and can become very expensive, very quickly. If you are unsure if you have a data package please contact your Departmental Telecoms Representative.

If you have a requirement to take your College mobile phone abroad then you must seek the express permission of your Line Manager to do so.

The College does not permit the transfer of the College SIM card from the supplied handset to another device. This may incur substantial cost for incorrect tariff usage and the College will seek full recompense for any additional charges incurred. Such action might also cause serious security breaches where the device carries confidential or sensitive College data.

To request a copy of your College mobile bill, contact your Telecoms Billing Representative.

4. RESPONSIBILITIES

The responsibility for the appropriate use of mobile devices rests with the designated user, their line manager and ultimately the relevant Head of Department.

Department/Line Managers are responsible for:

- determining eligibility of staff and appropriate mobile device(s) for their role;
- informing their staff members of their rights and obligations under this policy;
- arranging for recharges to be paid for mobile devices and usage bills prepared and issues monthly by ICT.

Telecoms Representative Responsibilities:

- Ordering appropriate mobile device(s) for staff from ICT, according to procedure;
- Monitoring the overall cost of every mobile device used by a member of the teams for which they are responsible;
- Justifying costs/usage of any user whose mobile usage/costs breach this policy;
- Reporting to ICT Services and line management any concerns regarding any abuse, misuse or breach of policy regarding any mobile devices.

User Responsibilities:

- Complying fully with legislation, this policy and related College policies;
- Appropriately securing the device(s) and information held on it;
- Deleting College information from the Mobile Device when no longer required or sooner if required by the College to delete it;
- Updating the device (where possible) so that it has an up-to-date operating system;
- College mobile devices must not be used to take photographs of an individual(s) without that individual's consent.
- Creation or transmission of material that infringes copyright is prohibited.
- Users must take reasonable care of College devices they receive. Please note that although protective cases and screen guards can prevent or reduce accidental damage they are not provided by College as standard issue.
- Users must not pass their mobile device(s) to others. At the end of their lifecycle, devices should be returned to the Telecoms Representative, who should return them to ICT to be properly decommissioned.

Users who are allocated a mobile device will be held responsible for the device and all calls made and other charges incurred. It is therefore essential that devices are always kept secure and not used by anyone other than the named individual. Users should take all reasonable and practical precautions to keep the device safe from damage, loss or theft. Devices should be set to automatically lock if inactive for 5 minutes or less.

The device's warranty does not include accidental damage, so care should be taken when using it. We do not have insurance to cover accidental damage. In circumstances where it has been shown that the employee's carelessness contributed to the loss of or damage to the device, then the employee may be required to contribute to the replacement or repair costs.

If you use mobile devices such as laptops, smartphones and tablets, whether personal or College-owned, to connect to the College network and access College's systems and data, you are personally responsible for keeping data secure. No sensitive data should be stored on a mobile or portable device unless it is encrypted. Mobile devices are just handy-sized computers, so they're not only attractive to thieves but are exposed to the same scam email, virus and malware risks as desktop computers.

There are ways you can protect mobile devices, e.g. use a PIN or password to restrict access, only install apps from trusted sources (e.g. Apple App Store, Google Play & Windows Store), do not open email attachments from unknown sources, do not click on links from unknown sources, keep software updates up to date, and, always keep your College device safe. If in doubt, contact ICT Service Desk for advice.

For more guidance to help you to protect mobile devices, keep data secure and stay safe online, visit **ICT's Be Secure website:** Protect mobile devices
If you misplace your mobile phone, you can request that an 'admin bar' is put on its number, which will render the mobile number unusable temporarily. Contact O2 by dialling 0844 826 0288 and request an admin bar. Once you have found your mobile, call the same number and ask for the admin bar to be removed. If your College mobile has been stolen you must report this to O2 immediately by dialling 0844 826 0288 and request an admin bar and report this to your Departmental

Telecoms Representative at the earliest opportunity. If the device is confirmed stolen, a permanent bar should be put in place to prevent future use.

All College mobile devices have a lower and an upper usage limit. This is a requirement of our auditors and helps mitigate costs in the event of a mobile being lost or stolen. When you reach your lower limit you will receive a text message advising that your usage is unusually high and you may find your service restricted. When you reach your upper limit your service will be barred and you will no longer be able to make calls, send text messages or mobile data services will be slower than normal (you will still be able to use Wi-Fi). By default, the lower limit is set to £200 per month and the upper limit to £300 per month."

However, as usage is received by O2 only once every 24 hours; during the course of each day, data usage information accrues and then downloads to the O2 billing platform at midnight. It is possible therefore to consume significant amounts of data in a single day, greatly exceed the £300 monthly limit and not receive any notification.

Should you need to get the high usage bar removed from your College mobile, contact your Telecoms Representative.

5. SAFETY

5.1 Using mobile communication devices in controlled or hazardous areas

If considering the use of any mobile device in a controlled environment or area where hazardous products or procedures are used, the activity must be carefully risk assessed and, if necessary, advice sought from the Area Controller or the Laboratory Manager, or the relevant College Safety Officer, or Estates Facilities' Head of Health and Safety.

In some hazardous or controlled areas, it may be necessary to ban the use of any mobile communication device. Strict adherence to local rules and any established Safe Systems of Work must be observed at such hazardous locations or sites, particularly in areas where an explosive atmosphere may occur (Ex zones), or in proximity to strong magnetic fields, e.g. Mass Spectrometry or Nuclear Magnetic Resonance (NMR) facilities.

5.2 Use of Mobile Devices when Driving

Use of mobile phones, hands-free mobile phones, or other hand-held devices is not permitted while driving. For more information see College's policy on 'Driving on College Business'.

Version History

Version/Status	Release Date	Comments
0.1/Draft	26 Oct 2017	Prepared by Stuart Kerr, reviewed by John Shemilt, Director of ICT.
0.2/Draft	05 Dec 2017	Reviewed by Okan Kibaroglu, Head of Governance, Heads of Sections in ICT and John Shemilt, Director of ICT.
0.3/In Review	10 Jan 2018	Reviewed by John Neilson, College Secretary
0.4/In Review	23 Mar 2018	Review by members of Information Governance Steering Group
1.0/Approved	28 June 2018	Section 1.2 'Scope' section added to clarify devices in scope as advised by Jon Tucker. Additions to Section 5 as advised by Julia Cotton. Approved by IGSG and ready to publish.