ISD Telephony Services Mobile Telephony Policy

DOCUMENT INFORMATION

Document Name: ISD Telephony Services Mobile Telephony Policy
Service: ISD Telephony Services
Author: Mike Turpin (MT)
Contributors: Bridget Kenyon (BK), Nicola Arnold (NA), Gavin McLachlan (GM) and Gary Sawyer (GS)
Issue Date: 30/07/2014

DOCUMENT HISTORY

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Summary of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>02/05/2014</td>
<td>Draft</td>
</tr>
<tr>
<td>0.2</td>
<td>15/05/2014</td>
<td>Incorporating comments from GM, NA, BK &amp; GS</td>
</tr>
<tr>
<td>0.3</td>
<td>16/5/2014</td>
<td>Incorporating amendments by MT</td>
</tr>
<tr>
<td>0.4</td>
<td>22/5/2014</td>
<td>Incorporating further comments from NA for submission to Board</td>
</tr>
<tr>
<td>0.6</td>
<td>9/06/2014</td>
<td>Incorporating comments from NA, BK &amp; GS</td>
</tr>
<tr>
<td>0.7</td>
<td>30/06/2014</td>
<td>Incorporating formatting and comments from MT and NA</td>
</tr>
<tr>
<td>0.8</td>
<td>09/07/2014</td>
<td>Incorporating with comments from NA/BK and approved by Rex Knight</td>
</tr>
</tbody>
</table>

This document may include information that is CONFIDENTIAL and shall not be disclosed outside UCL and shall not be duplicated, used or disclosed, in whole or in part, for any purpose other than to evaluate and implement procedures defined within this document.

Contents

1. POLICY INTRODUCTION AND OVERVIEW ................................................................. 2
   1.1 Aims of the policy ............................................................................................ 2
   1.2 What does the policy cover? ............................................................................. 2
2. UCL MOBILE TELEPHONY POLICY ........................................................................ 3
   2.1 Charges ............................................................................................................. 3
   2.2 Personal Use .................................................................................................... 3
   2.3 Usage Monitoring ............................................................................................. 4
   2.4 Security ............................................................................................................. 4
   2.5 Lost or Stolen Devices ..................................................................................... 5
   2.6 Leavers .............................................................................................................. 5
   2.7 Driving and Operating Machinery .................................................................... 5
   2.8 Where NOT to use your phone other than driving ......................................... 6
   2.9 Conduct and Responsible Use ........................................................................ 6
1. POLICY INTRODUCTION AND OVERVIEW

UCL has procured a managed mobile service from Abzorb Services Ltd. who are the supplier for all mobile services. All requests for new mobile devices must be submitted via the UCL ordering portal provided by Abzorb at: [http://ucl.abzorbshop.co.uk](http://ucl.abzorbshop.co.uk). It is also intended that all existing mobile phone contracts, both centrally managed and individual or departmental accounts, will be migrated to the preferred supplier.

The old policy is out of date and doesn’t take into consideration that the majority of phones are now “smart phones” which are really mobile computers, they are no longer just a voice and text device. We should consider the ability for these devices to be transmitting virtually non-stop and having some presence on networks, which can introduce safety and security issues.

1.1 Aims of the policy

The policy aims to set out fair use of mobile hardware supplied by UCL and to make recommendations on safe and secure use for those using their own mobiles at UCL. Attention should be paid to the risks of using a mobile phone and the fact that most smart phones these days can transmit and receive many frequencies at varied powers. Consideration should also be given to mobile security and the recommendations in the policy aim to reduce the risk of information security breaches and/or data loss.

Provision of a mobile device, by UCL, should not be assumed for all posts, but when required in order to carry out the duties of a post, or as agreed by the Head of Department, Faculty or appointed authority. UCL expects users to safeguard the hardware at all times, the data contained on the device and to use the device in a safe and responsible manner.

Failure to comply with this policy may result in disciplinarily action being taken in line with UCL’s HR policy.

1.2 What does the policy cover?

The policy covers mobile device usage, security, safety, individual responsibilities and finance – But is not meant to obstruct the effective use of mobile phones and the benefits they can bring. It is intended to provide a balance between an excellent communication tool and safety, security and responsibility.

Although the policy is aimed at UCL issued mobile devices, some of the recommendations will also be applied to personal devices brought to UCL. Please note that all personal devices used to access UCL email and/or connected to UCL networks and systems, must comply with the security section below.
2. UCL MOBILE TELEPHONY POLICY

2.1 Charges

2.1.1 Abzorb Services Ltd are UCL’s supplier for mobile services and all purchases of hardware (handsets, chargers, MiFi puck etc.), new contracts, billing and support will be via Abzorb.

2.1.2 From 1 August 2014, new mobile device purchases, usage and rental charges cannot be reclaimed on expenses, paid through an invoice processed outside of ISD or charged to a UCL credit card. Contracts taken out before this date may be claimed, if approved by the School Finance Director, and if the contract is in the name of UCL. Business calls must be claimed on non-UCL equipment in line with UCL’s Expenses Policy (see link to Policy on website; http://www.ucl.ac.uk/finance/expensespol/index.html).

2.1.3 When choosing a handset, users should ensure that the most appropriate handset is purchased along with a standard contract. This should be the lowest cost which will deliver the necessary functionality required for the member of staff to undertake their duties. Handsets will not automatically be replaced at the end of a contract period, unless the handset is in some way faulty. Handsets should not be upgraded every time a new handset is made available from a provider and certainly not within the contract period.

2.1.4 Overseas roaming will be switched off for all handsets and contracts as supplied and may only be switched on with approval from the relevant School/Professional Services Finance Director. Streaming data abroad can be very expensive and any unauthorised use will be charged back to the user.

2.1.5 Special care should be taken when using your mobile abroad. Bolt-ons will be applied if you are an authorised international user, but the cost will quickly mount up, especially if you exceed your data limits. For those reasons UCL requests that use abroad is limited to 14 days as a maximum and data is not streamed abroad. Where extended stays abroad are required for your role it will be cheaper to purchase a SIM card for that country and ISD Telephony can offer advice, please contact telecoms@ucl.ac.uk.

2.2 Personal Use

2.2.1 Mobile equipment issued by UCL must be used primarily for work-related communications and activities. Inland Revenue guidance does permit an employee who has been issued with a business mobile to make private calls, but only when private use is “not significant”. (See http://www.hmrc.gov.uk/manuals/eimanual/EIM21779.htm for more details.)

2.2.2 Use of, or subscription to, premium and/or interactive mobile services using a UCL phone is strictly prohibited. This includes (but is not limited to) the downloading or forwarding of ring tones, videos and mobile-TV. Call and data use will be monitored on a regular basis. Where personal use is excessive, departments are permitted to require a contribution to be made by the individual.
2.2.3 SIM Swapping – UCL does not permit the transfer of the SIM card from the supplied handset to a personal device or from a mobile phone to iPad or Tablet. This may incur substantial costs for incorrect tariff usage and the University will seek full recompense for any additional charges incurred due to this action. The University would also point out that this may cause serious security breaches where ‘data’ based devices carry University information.

2.2.4 Voicemail should be set up and maintained at all times on UCL issued mobiles unless impractical due to role or disability.

2.3 Usage Monitoring

2.3.1 Call records for UCL provided mobile devices will be made available by the supplier to Finance and ISD Telephony Services who will have access to all call details (numbers dialled, duration, cost etc.). Departmental Administrators, Heads of department and/or the budget holders will be able to check detailed call records for their departments in order to monitor usage and spend; individual users will also be able to check their own usage.

2.3.2 Monitoring usage allows ISD Telephony Services to check on contract performance, drive down costs and make savings on frequently used call routes, it will also be used to identify improper and excessive use.

2.3.3 Please note that call records refers to usage statistics and details, not the actual recording or monitoring of any calls, data or voicemail.

2.3.4 Monitoring and recording of the mobile phone location information is not part of this policy. UCL reserves the right to use location information for specific purposed, at the user’s discretion.

2.4 Security

2.4.1 It is mandatory that all devices be protected with a 4 digit PIN as an absolute minimum with six digits or more being preferable or a substantial password. The password or PIN can be written down on paper by the user, put the paper in an envelope, seal it and sign over the seal. The envelope should be put in a secure location. In an emergency, the admin can indeed get hold of the password/PIN; but otherwise, the user is assured that the admin is not casually using their password/PIN to access their phone. Where staff changes are involved, the phone should be wiped and reissued as a new phone, not “inherited” with all personal data still on it. Biometric security options (e.g. fingerprint login) should be evaluated to identify whether they are effective, as some solutions are easily bypassed or spoofed.

2.4.2 It is highly recommended that encryption, if available on your device, is enabled to protect your data and UCL data contained in emails, documents, etc.

2.4.3 Software downloads and Apps should only be installed from authorised sources (i.e. Google Play, Apple App Store, etc.) Apps from unauthorised sources can contain viruses and malware that could compromise the security of the mobile device as well as the security of UCL networks and systems.

2.4.4 Devices must not be “jailbroken” or otherwise altered to allow unauthorised configuration.
2.4.5 Remote wipe should be configured to enable personal and corporate data (email, etc.) to be erased remotely should the device be lost or stolen.

2.4.6 All use of mobile phones to access UCL data (including email, etc.) must comply with the UCL Information Security Policy:
http://www.ucl.ac.uk/informationsecurity/policy/public-policy/Data_protection_policy_ISC_20110215

2.4.7 Connecting a mobile device to the UCL network must comply with the UCL Policy on connecting equipment to the college network:
http://www.ucl.ac.uk/informationsecurity/policy/public-policy/Connection_ISC_200811

2.4.8 The use of UCL email on a mobile device must comply with the UCL Policy on Electronic Mail: http://www.ucl.ac.uk/informationsecurity/policy/public-policy/E-mail_ISC_200912

2.4.9 Users of UCL issued mobile devices should be aware that these devices may be subject to monitoring and/or seizure in the event of a security incident, in accordance with the UCL Policy.

2.4.10 The person to whom the phone has been issued is responsible for ensuring compliance with the above policies, and is responsible if a breach occurs.

2.5 Lost or Stolen Devices

2.5.1 Lost or stolen devices must be reported to your service provider at your earliest opportunity.

2.5.2 UCL issued devices should be reported to ISD Telephony 24h Service Desk: 01484 405300. Please obtain a reference code for your service call.

2.5.3 Failure to report your phone may result in additional charges from the service provider as they can only act from the moment you advise them of the loss.

2.5.4 Unwanted or mobile devices that have been replaced must be returned to ISD Telephony Services to ensure Asset Registers are updated and the correct legislative disposal procedures are followed.

2.5.5 Where devices are lost, UCL reserves the right to charge individuals for the cost of a new handset.

2.6 Leavers

2.6.1 UCL issued mobile devices must be returned when an employee leaves UCL employment.

2.7 Driving and Operating Machinery

2.7.1 No person driving a vehicle (including heavy plant and industrial machinery, whether mobile or stationary in use i.e. a mobile platform or scissor lift or any situation where a distraction is likely to cause harm) is allowed to use a mobile phone in any way. Devices must also be muted or switched off in other situations where concentration is paramount to safety. The telephone user has a duty of care whether the phone is UCL issued or a personal handset.
2.8 Where NOT to use your phone other than driving

2.8.1 There are some areas where devices need to be switched off; e.g. on an aeroplane. Unless your phone can be set to ‘Airplane Mode’ it should be switched off when advised to do so.

2.8.2 Do not take your telephone abroad or use roaming unless you have specifically cleared this with your Line Manager and Departmental Administrator.

2.9 Conduct and Responsible Use

2.9.1 At all times, mobile devices should be used in a manner that is professional, morally acceptable and above all, respectful to others.

2.9.2 Mobiles should not be used in; meetings, seminars, lectures, some laboratories, hospitals, the cinema or anywhere with a quiet area specified by signage. If you are on-call or providing an emergency response then a muted device or one set to vibrate may be acceptable, but calls should not be taken in the prescribed quiet area.

2.9.3 If the area has a mandatory ban on mobile use then you should turn it off whether on-call or not or leave the area. Many departments/buildings have local rules regarding the use of mobile phones, and these must always be respected. If an area is a designated mobile free area, do not use your phone, even to send messages or emails.

2.9.4 Recordings of any kind (audio, video or pictures) are not allowed unless it is a public area or capturing mechanical or electrical failures with equipment or you have permission or the right to photograph the subject or material. As previously mentioned, to avoid people feeling vulnerable phone use is not recommended where it could impede the dignity of others; e.g. changing rooms, toilets, showers, bathrooms, sleeping areas, or anywhere which may be deemed sensitive.

2.9.5 You are responsible for your device and the content upon it. No mobile devices should be brought on to UCL property or connected to UCL networks (including wireless) that contain inappropriate content, this includes Apps, wallpapers, ringtones and notifications.

2.9.6 For users who have a UCL issued device it is your responsibility to ensure it is maintained carefully and looked after on a day to day basis.

2.9.7 When bringing your own devices to UCL you should be aware that UCL accepts no responsibility for the use, repair or maintenance of that device. For a UCL issued device the same rules apply as for any other supplied device or tool as part of your role.

2.9.8 It is your responsibility to ensure the device is not used to harass or bully anyone, abuse, insult or attack anyone in any way, incite hatred in any form, is not used for racist or sexist activity, for chain letters or games and not used to obtain or transmit pornography or used in any criminal activity. Copyright breach of video, music, images or written word is unacceptable.