BUCKINGHAMSHIRE
NEW UNIVERSITY
EST. 1891

MOBILE DEVICE USE POLICY

bucks.ac.uk

Contents

Approved by:	**IS&T Director**	Date first published:	**Jan-2015**
Version No.	**5.0**	Date updated:	**Oct-2019**
Owner:	**IS&T**	Review Date:	**Jun-2022**

This document has been designed to be accessible for readers. However, should you require the document in an alternative format please contact the Academic Quality Directorate.

Introduction

1 Bucks New University provides mobile phones and other mobile devices to staff members and business functions where there is a demonstrated business need. The purpose of this document is to establish guidelines regarding eligibility, usage and management of University owned mobile services.

Policy Scope

2 This policy applies to all mobile devices financed by the University and any personal devices that are used to receive University business.

Policy Intent

3 This policy is produced to provide a clear instruction on: the authorisation and usage of mobile devices; guidance on safety and security; and to limit any financial and corporate liability for the University's telecommunications.

Policy Provisions and Principles

Eligibility

Individual Staff Members

4 Bucks New University will provide an appropriate mobile device to those members of staff where it is deemed necessary for the execution of the duties of their position.

Other individuals

5 Mobile devices will not normally be issued to students, contract employees, temporary staff or consultants. Any other requests must be submitted with an appropriate business case.

Business Functions

6 There are occasions where a mobile device will be allocated to a business function rather than an individual, especially to align with the Health and Safety Policy. These devices will be used by a group of people as necessary. The mobile device will be issued to one member of the team (Head of Department/Manager) who will be responsible for ensuring that its use and security complies with this policy.

Issuing Mobile Devices

7 The University offers a limited range of mobile devices and tariffs which are allocated and supported by the Information Systems and Technology (IS&T) Directorate.

8 All mobile device requests must be made through the IS&T Directorate using the appropriate application form. The purchase of a device and associated airtime contract will need to be authorised by the relevant Line Manager and/or Head of Department before it is issued by the IS&T Directorate.

9 The most appropriate device and tariff combination will be determined on the basis of information contained within the application form. Handset allocation is determined on the basis of cost effectiveness not personal choice.

10 Requests for non-standard mobile phones and contracts will only be met when there is a clear business need e.g. where specialised mobile phones are required for research purposes or for particular non-research related activities or as a reasonable adjustment for any staff member with specific requirements due to a disability. Purchases falling outside standard mobile phones and/or preferred supplier guidelines will be treated as a hardware purchase and may need to be paid for by the business area.

11 The device will need to be signed for by the employee it is issued to. Users must not under any circumstances re-allocate mobile devices to others without first seeking authorisation from the IS&T Directorate. In the event that the IS&T Directorate authorise the reallocation of a device to another individual, all elements of the contract, including the phone number, will be transferred.

Mobile Data Device Usage

12 Voice and data mobile equipment issued by the University is for business purposed only. Personal usage should be kept to a minimum and be reimbursed to the University. Inland Revenue guidance does permit an employee that has been issued with a business mobile to make private calls, but only when private use is 'not significant'.

13 Use of or subscription to premium and/or interactive mobile services using a University phone is strictly prohibited. This includes (but is not limited to) the downloading or forwarding of ring tones, videos and mobile-TV. Failure to comply with this may result in disciplinarily action being taken against an employee.

14 Text messaging is permitted via a University mobile phone, subject to similar limitation to voice calls. Users should be aware that each text message sent carries a cost and therefore, must not be used as a 'chat medium'. Text messages must be business related only unless otherwise authorised.

15 The creation or use of a personal account, such as an AppleID or Microsoft Hotmail/Outlook account, is prohibited on University issued mobile data devices.

16 The University does not permit the transfer of the University SIM card from the supplied mobile device to a personal device. 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. It should also be noted that this may cause serious security breaches where 'data' based devices carry University information.

17 All users and their line managers must be aware that contracts will be reviewed and call usage will be monitored on a regular basis.

User Responsibilities

18 Members of staff who are allocated a mobile device will be held responsible for the handset, all calls made using the device and other charges incurred. It is therefore essential that devices must be kept secure at all times and use by anyone other than the named individual is prohibited.

19 Sensitive information (e.g. personal data, passwords, or any other data that could bring the University into disrepute should it fall into the wrong hands) should not be stored on an

unsecured mobile device. Staff should consider the impact of retrieving their email on mobile devices.

20 Mobile devices remain the property of the University at all times and must be surrendered along with any accessories when a member of staff leaves employment or on demand by the Head of Department, HR or the IS&T Directorate.

21 If the device is no longer needed, or an employee is leaving it must be returned, along with any accessories, to the IS&T Directorate.

22 Depending on the contract, allowance is made for reasonable use as an inclusive charge. Included in most of the phone contracts is an allowance for reasonable usage. Exceptional high usage charges exceeding this limit are made by the service provider. If it is felt that excess charges do not represent reasonable usage, the user may be asked to refund the University.

23 The individual user is responsible for providing the IS&T Directorate, all data relating to the user of the mobile device whenever any relevant details are changed.

24 If the device is allocated to a different user for any reason, the device must be taken to the IS&T Directorate, who will wipe all the previous user's information and configure the device for the new user.

25 The user will be charged for missing mobile device accessories (e.g. cables and chargers) if they are not returned to the IS&T Directorate with the device when it is no longer needed.

26 University mobile devices must not be used for the purpose of illegal transactions, harassment, obscene behaviour or any other activity that would breach any University policy.

27 Employees must not use a University mobile device while operating a motor vehicle unless it is fitted with a hands-free kit and will be responsible for any fines incurred as a result of traffic regulation breaches.

Replacing an Existing Device

28 The University will replace the device where there is a justified reason in conjunction with any third party service provider. In circumstances where it has been shown that the employee's lack of care contributed to the loss of or damage to the device, then the employee may be required to contribute to the replacement cost.

Monitoring

29 Summary usage reports are regularly reviewed by the IS&T Directorate for the purpose of monitoring compliance with this policy. Excessive usage or expensive calls can be automatically flagged up by the network provider. The IS&T Directorate will check the appropriateness of the usage with the Line Manager or Head of Department and itemised bill can be issued if requested.

30 Where unauthorised calls have been made the user will be asked to reimburse the University (Itemised bills for an individual mobile phone will be made available to the direct Line Manager or Head of Department where there is reasonable suspicion of misuse). The user will be expected to pay for any personal calls/text messaging.

Security

Physical

31 Unattended mobile computing devices must be physically secured. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

Software

32 Devices must not be connected to a PC or Mac which does not have up-to-date and enabled anti-malware protections and which does not comply with University policy.

33 Devices must not be “jailbroken” or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

34 Only applications approved by the IS&T Directorate may be installed on mobile devices. Installation of code from untrusted sources is forbidden as is the loading of pirated software or illegal content. If you are unsure if an application is approved contact the IT Service Desk.

Passwords

36 Each device is provided with a password/pin facility securing access which must be enabled at all times as a minimum security measure.

Loss of Device

37 Loss or theft of any device used for business purposes must be reported to the IS&T Directorate by the user immediately. This may help to prevent unauthorised usage of the device and possible breach of the University’s Policy for the use of IT facilities and systems. If necessary, the device can be remotely wiped.

Key Relevant Documents

Data Protection policy

Information Security Policy

Acceptable Use Policy