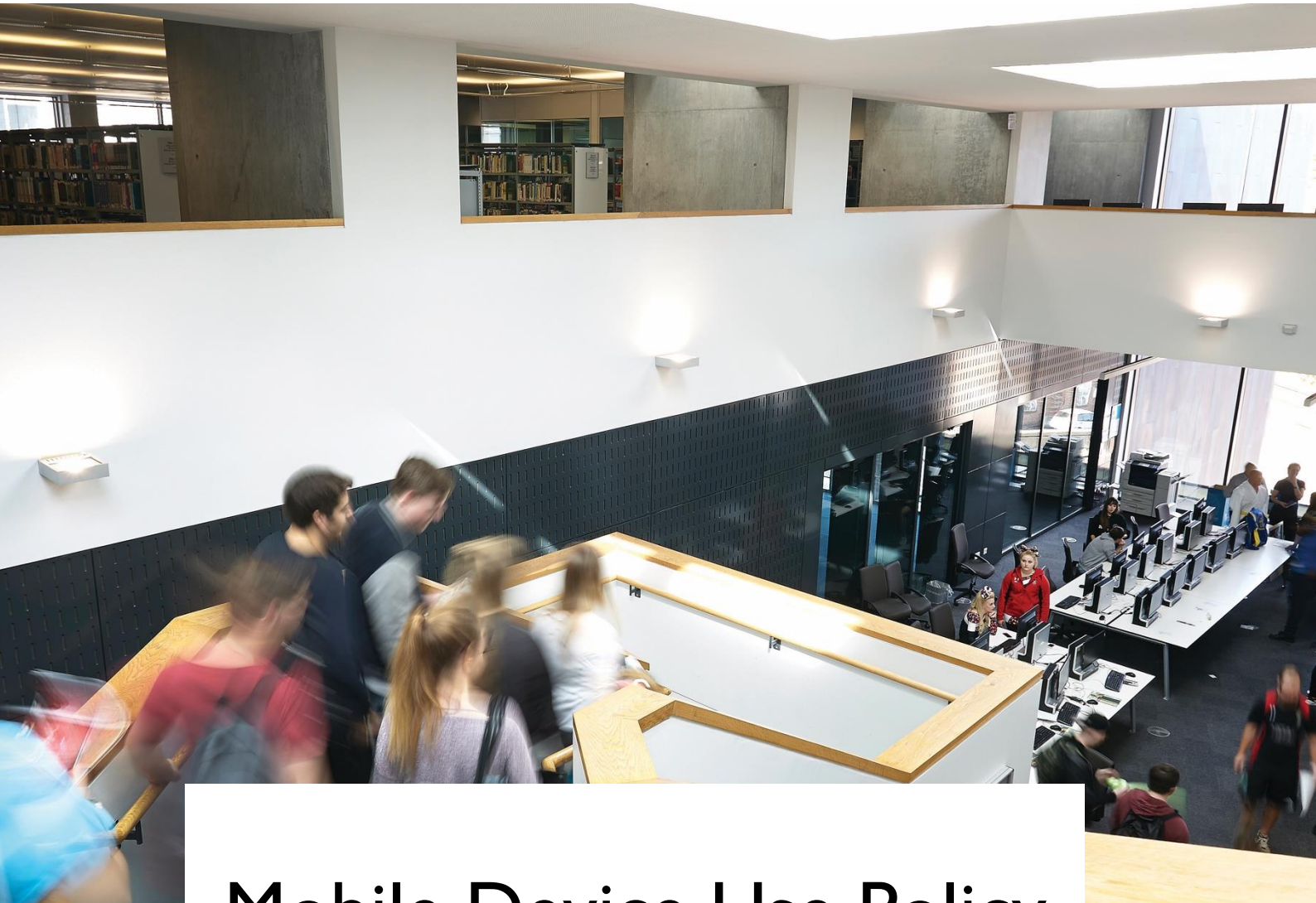




BUCKINGHAMSHIRE
NEW UNIVERSITY

EST. 1891



Mobile Device Use Policy



Contents

Purpose.....	4
Applicability and Scope.....	4
Eligibility.....	4
Business Functions.....	4
Issuing Mobile Devices	4
Mobile Data Device Usage	5
User Responsibilities	5
Replacing an Existing Device	6
Monitoring.....	6
Physical Security	6
Software Security	6
Passwords.....	7
Loss of Device	7
Enforcement	7
Key Relevant Documents.....	7

Approved by: Digital Experience Steering Group
Version: 6.0
Owner: Director DTS

Date first published: Jan-2015
Date updated: Oct-2023
Review Date: Oct-2026

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

© Buckinghamshire New University

Purpose

- 1 Buckinghamshire New University (BNU) 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.
- 2 This policy is produced to provide a clear instruction on: the authorisation and usage of mobile devices and guidance on safety and security to limit any financial and corporate liability for the University's telecommunications.

Applicability and Scope

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

Eligibility

- 4 **Individual Staff Members.** BNU 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.
- 5 **Other individuals.** 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 (e.g., Head of Directorate) 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 Digital and Technical Services Directorate (DTS).
- 8 All mobile device requests must be made through DTS 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 Directorate or Academic School before it is issued by the DTS.
- 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 DTS. In the event that DTS 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 purposes 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 disciplinary 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 Directorate or Academic School, HR or DTS.
- 21 If the device is no longer needed, or an employee is leaving it must be returned, along with any accessories, to DTS.
- 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 DTS with 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 DTS, 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 DTS 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 DTS for the purpose of monitoring compliance with this policy. Excessive usage or expensive calls can be automatically flagged up by the network provider. DTS will check the appropriateness of the usage with the Line Manager or Head of Directorate or Academic School 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 Directorate or Academic School where there is reasonable suspicion of misuse). The user will be expected to pay for any personal calls/text messaging

Physical Security

- 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 Security

- 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 DTS 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

- 35 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

- 36 Loss or theft of any device used for business purposes must be reported to DTS by the user immediately. This may help to prevent unauthorised usage of the device and possible breach of the University's Acceptable Use Policy. If necessary, the device can be remotely wiped.

Enforcement

- 37 Any actual or suspected breach of this policy must be reported to the Director of DTS via the Service Desk. The Director of DTS will take appropriate action and inform the relevant internal and external authorities.
- 38 Failure to comply with this policy may result in disciplinary action in accordance with the relevant process.

Key Relevant Documents

- 39 This policy should be read and understood in the context of other Buckinghamshire New University Policies which together form the Information Security framework. Key documents include:
- Applicable Laws and Regulations
 - Acceptable Use Policy
 - Data Protection Policy
 - Information Security Policy

Appendix: Equality Impact Assessment

1. What is changing and why?				
The current policy is being reviewed to ensure that it remains up to date and compliant with all legislative requirements.				
2. What do you know?				
This policy is a factual and procedural document, providing detailed standards for issuing mobile phones and other mobile devices to staff members and business functions. It also establishes the rules for how mobile devices are used and secured within the University.				
3. Assessing the impact				
	Could benefit	May adversely impact	What does this mean? <i>Impacts identified from what you know (actual and potential)</i>	What can you do? <i>Actions (or why no action is possible) to advance equality of opportunity, eliminate discrimination, and foster good relations</i>
a) How could this affect different ethnicities? <i>Including Gypsy, Roma, Traveller, Showmen and Boaters, migrants, refugees and asylum seekers.</i>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	This policy does not distinguish between or affect differently people of different ethnicities. It protects the interest of all users.	The policy supports equality and diversity by providing information on how any member of staff can request a university issued mobile device.
b) How could this affect cisgender and transgender men and women (including maternity/pregnancy impact), as well as non-binary people?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	This policy does not distinguish between or affect differently cisgender and transgender men or women or non-binary people. It may have a positive impact on those users who wish to take advantage of flexible and or dynamic working practices.	The policy supports equality and diversity by providing information on how any member of staff can request a university issued mobile device.
c) How could this affect disabled people or carers? <i>Including neurodiversity, invisible disabilities and mental health conditions.</i>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	This policy does not affect disabled people or carers. It may have a positive impact on those users who can only access University resources remotely. It protects the interest of all users.	The policy is available on the BNU website therefore is available in different fonts, text size and through assistive technology. Staff users with a disability are able to request a different type of mobile device if the ones available do not meet their specific needs for example a device that allows the text size to be altered or support for voice commands. This will be regularly reviewed to ensure the devices BNU purchases are suitable for all different types of user.
d) How could this affect people from different faith groups?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	This policy does not distinguish between or affect differently people from different faith groups. It protects the interest of all users.	

e) How could this affect people with different sexual orientations?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	This policy does not distinguish between or affect differently people with different sexual orientation. It protects the interest of all users.	
f) How could this affect different age groups or generations?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	This policy does not distinguish between or affect differently people from different age groups or generations. It protects the interest of all users.	It is acknowledged that different age groups will have different capabilities, experience and technical skills when using mobile devices. Additional guidance will be available to those who require additional support in using a university issued mobile device if it is a requirement of their role.
g) How could this affect those who are married or in a civil partnership?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	This policy does not distinguish between or affect differently unmarried or married people or those in civil partnerships. It protects the interest of all users.	
h) How could this affect people from different backgrounds such as: socio-economic disadvantage, homeless, alcohol and/or substance misuse, people experiencing domestic and/or sexual violence, ex-armed forces, looked after children and care leavers.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	This policy could have a positive impact on those individuals who find it difficult to attend University in person or for whom mobile or internet access is the only way that they access University resources.	
i) How could this affect people with multiple intersectional experiences?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	This policy applies to all in the same way therefore there will not affect those with multiple intersectional experiences.	
4. Overall outcome				
No major change needed <input checked="" type="checkbox"/>	Adjust approach <input type="checkbox"/>	Adverse impact but continue <input type="checkbox"/>	Stop and remove <input type="checkbox"/>	
5. Details of further actions needed				
The inappropriate use of the Policy will be managed in accordance with the University's policies and procedures and reported to external bodies when appropriate.				
6. Arrangements for delivery and future monitoring				
The policy will be reviewed every three years. The Director of Digital & Technical Services is responsible for reviewing the policy.				
7. Completed by:	Jenny Horwood	Technical Project Manager	Date	04-Oct-23
8. Signed off by:	Nicholas Roussel-Milner	Director DTS	Date	21-Dec-23



High Wycombe Campus
Queen Alexandra Road
High Wycombe
Buckinghamshire
HP11 2JZ

Aylesbury Campus
59 Walton Street
Aylesbury
Buckinghamshire
HP21 7QG

Uxbridge Campus
106 Oxford Road
Uxbridge
Middlesex
UB8 1NA

BNU based at
Pinewood Studios

Pinewood Studios
Pinewood Road
Iver Heath
Buckinghamshire
SL0 0NH

Missenden Abbey
London Road
Great Missenden
Buckinghamshire
HP16 0BD

Telephone: 01494 522 141

 BucksNewUni

 BucksNewUni

 BucksNewUni

 BucksNewUniversity