Policy on the acquisition, use and transfer of Mobile Phones, and related tariffs

1 Purpose

1.1 To ensure that any contract for the provision of mobile phones for legitimate University business purposes is taken out with the University's sole contracted supplier, as detailed in the guidance document.

1.2 To ensure that the most cost-effective handset and tariff is selected and that this remains appropriate throughout the life of the contract through periodic tariff checks

1.3 To ensure that the purchase and use of all mobile phones in support of the University's legitimate business purposes is correctly assessed, authorised and managed.

1.4 To establish expectations and allocate responsibilities for all University mobile phone users

1.5 To ensure that all mobile phone purchases are controlled and managed centrally by Digital Technology Services.

1.6 To ensure that users of mobile phones follow the University's information security policies and undertake appropriate training.

2 SCOPE, ELIGIBILITY AND TYPE OF MOBILE PHONE

2.1 The business need for any University member of staff to have a mobile phone must be justified by the role and responsibilities of that member of staff.

2.2 Each request will be assessed by the user's line manager and authorised by the line manager registered in the HR system.

2.3 Upgraded/replacement devices will only be authorised when a mobile phone is no longer fit for use or

The assessment must be made against the criteria set out below.

How necessary the mobile phone is for the purposes of the member of staff's legitimate University work within normal working hours and/or outside normal working hours.

The requirement for the member of staff to spend a proportion of time away from their desk. Staff who travel on business or work outside, lone workers etc, may be justified in having a mobile phone.

3 Responsibilities and Ownership

Digital Technology Services (DTS)	Ensuring suitable devices are available for users. DTS will not provide advice or guidance on technical specification of devices The mobile device will be logged and registered by DTS against the member of staff on the University's asset management system. Devices no longer required will be sent to Academia in line with the Reuse and Recycle Policy any device not suitable for the scheme will be securely disposed of. DTS does not accept any responsibility for data left on a device given to Academia for disposal
Heads of Schools, Functions and Departments	Ensuring that their staff are made aware of this policy and that breaches of it are dealt with appropriately. Head of School, Head of Directorate or equivalent are responsible for ensuring that any transfer does not result in any unauthorised disclosure of personal data or sensitive information and complies with the University's policies on data protection and information security generally. Returning a mobile phone back to DTS for disposal does not terminate the tariff. Mobile phones contracted for legitimate University purposes must be returned to the School, department or equivalent when a member of staff leaves the University or there is a change in role such that the staff member no longer requires the use of a mobile phone. The University will look to recover costs from either the member of staff or the School, department or equivalent if the phone is not returned The responsibility for the return of the handset rests with the Head of School, department or equivalent.
University staff	University staff are responsible for:

	Complying with this policy.

4 Consequences of Non-compliance

4.1 The University is bound by the General Data Protection Regulation (the GDPR) and the Data Protection Act 2018 (the DPA). The seventh principle the DPA states that:

> “appropriate technical and organisational measures shall be taken against accidental loss or destruction of, or damage to, personal data”

4.2 Loss of devices holding University data may cause damage and distress to those who entrust us to look after their data, damage the University’s reputation and its relationship with its stakeholders (including research funders), and have significant legal and financial consequences. The Information Commissioner can impose serious monetary penalties on the University for breaches of the GDPR and DPA.

4.3 Loss of devices containing other University data may give rise to loss of rights in intellectual property, inability to register rights in intellectual property and breach of contractual and other obligations to third parties for disseminating or otherwise failing to protect confidential information.

4.4 Failure to comply with this policy may result in us revoking your access to the University’s systems, whether through a device or otherwise. It may also result in disciplinary action being taken against members of staff up to and including dismissal. This will apply whether the breach occurs during or outside normal working hours and whether or not use of the device takes place at your normal place of work. You are required to co-operate with any investigation into a suspected breach, which may include providing us with access to the device.

5 Guidance and Key Principles

5.1 The following key principles underpin this policy statement. All staff must comply with these principles.

5.2 The contents of our systems and University data remain University property. All materials, data, communications and information, including but not limited to, e-mail (both outgoing and incoming), phone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device during the course of your work for the University or on its behalf is the property of the University, regardless of who owns the device.

5.3 University data held on personally owned devices is subject to the Freedom of Information Act and Data Subject Access rights under the GDPR and the DPA and must be provided to IMPS on request.

5.4 Use the authorised remote access facilities to corporate systems (e.g. Purchase to Pay and Employee Self-service) that are both secure and encrypted to access High Risk Data on the central servers instead of transporting it on mobile devices and portable media.

5.5 Do not keep any information longer than is necessary and only in line with University Record Retention guidelines. Avoid duplication of information wherever possible.

5.6 Any use of a personal device for or in connection with University work must be carried out in accordance with the University's procedures relating to equal opportunities, harassment, safeguarding, the Prevent duty, use of social media, intellectual property and with any relevant laws.

5.7 Members of staff are only allowed to have a maximum of two phone numbers registered in their name. One mobile phone number (for a handset) and one data number (for an iPad or tablet). Therefore, staff are only allowed one mobile phone handset at any one time.

5.8 Understanding the mobile device shall remain the property of the University of Reading

5.9 Due to information security issues, mobile phones will only be transferred to other members of staff following authorisation from the Head of School, Directorate or equivalent

Members of staff are expected to use the phone in a responsible manner. Schools and Departments will be liable for the continuing contracted line rental costs incurred, regardless of any loss of, or damage to, the mobile phone

If the mobile phone is legitimately transferred to a different member of staff, DTS must be informed of the detail by completing the Change of User form available through the DTS Self Service Portal.

All mobile phones should be reset back to factory settings and any personal log in (Apple or Google login) details removed from the device.

All members of staff who are issued with a mobile phone must observe Health and Safety Policy note 22 and the Driving for Work Policy and Procedures.

Members of staff are only allowed to have a maximum of two phone numbers registered in their name. One mobile phone number (for a handset) and one data number (for an iPad or tablet). Therefore, staff are only allowed one mobile phone handset at any one time.

Due to the high charges, members of staff should not subscribe to any text subscription services.

Personal Calls

University mobile phones should not be used for personal use.

Use Abroad (roaming)

The current contracted tariff allows for international data usage, this is limited to 20Gb of data shared between international travellers, excess data will be charged in increments of 1gb of data to the University.

International cellular connections are not as good as we are used to in the UK, and can result in users experiencing connection problems, these are outside of UoR control, often manually searching for a local network will be sufficient to resolve any connection problems.

Using Wifi data connections are always recommended where possible whilst roaming to minimise the usage charges to the University.

Switch off cellular data if not required

Switch off data roaming when not in use.

Buy a local sim card if travelling for long periods of time

If a strong and reliable wifi signal is present use MS Teams. Teams App would need to be downloaded before travelling. Teams needs a wifi connection rather than cellular for making and receiving calls, so should not be relied on.

6 Managing Mobile Phones

6.1 The mobile phone holder is responsible for ensuring that the phone is used in an appropriate manner: this includes numbers called, websites visited and applications used. The mobile phone holder is responsible for ensuring that they have completed the University's information compliance training (see above).

7 Early termination of mobile phone contracts

7.1 Should the termination of a contract become necessary prior to expiry of the original contract term, for example if a member of staff leaves the University and the phone is no longer required, the obligation to pay for the contract up to date of expiry will be the responsbility of the School, function or equivalent.

7.2 Where possible and appropriate, the mobile phone should be given to another eligible member of staff to avoid cancellation charges.

8 Replacement of lost mobile phones

8.1 Any loss of a mobile phone must be reported as soon as possible to DTS so that it can be barred from use. The Data Protection Officer should also be informed – imps@reading.ac.uk

8.2 Replacement mobile phones may be charged at full cost to the School/Service.

9 Requirements

9.1 Control access to the device (use touch or face ID if available, otherwise by password or PIN if neither touch/face ID nor password is possible). Passwords must meet the University's minimum password requirements (details available from the DTS Self Service Portal).

9.2 Use a screen or device lock that will trigger after a short period of inactivity (no longer than 10 minutes).

9.3 Keep your device's software up to date. This includes operating systems, applications, and anti-virus and malware protections.

9.4 Staff must not install untrusted apps: “Jailbreak” or “root” their mobile phone; or leave Bluetooth (or Near Field Communication, NFC) running if it is not needed, as these actions may compromise the phone.

9.5 Any apps installed must be for work purposes only.

9.6 On leaving the University, ensure all University data is deleted securely from your device. Ensure that master copies of documents that are required by the University are transferred to other University staff before you leave.

9.7 Remove University data from the device before disposing of the device or selling it or passing onto another individual. Ideally, the device should be reset to factory defaults.

9.8 If you are accessing UoR data, do not leave your device unattended in situations where others could access it and ensure it is physically secure at all times. Do not share your device with others, including members of your household.

The loss or theft of a University mobile phone must be reported immediately in accordance with the University Security Incident Response Policy and Procedures.

9.9 Ensuring that University data is removed from the device before disposing of the device by returning it to DTS for disposal

9.10 Do not process or view High Risk Data in public places

10 Related policies, procedures, guidelines or regulations

Key related policies and rules:

- Data Protection Policy
- Information Security Policy
- Regulations for the Use of the University of Reading’s IT Facilities and Systems
- Encryption Policy
- Remote and Mobile Working Policy
- Mobile Device Management Policy
- Guidance on Remote Working
- Policy on the Acquisition, Use and Transfer of Mobile Phones
- IT Equipment Disposal Policy
- Code of Practice on Intellectual Property
- Equal Opportunities
- Information Security Incident Response Policy

11 Review

11.1 This Policy shall be reviewed at regular intervals and documented within the version history. Reviews will take place as a minimum at the documented frequency and in the event of any of the below:

- Significant change in University operations
- Significant change in legislation, regulatory requirements, industry guidance or similar

- In the event of a compromise of data protection or security where the content or compliance with this policy is identified as an aggravating or mitigating factor
- Any other identified requirement necessitating substantive changes ahead of scheduled review

11.2 Substantive changes shall be reviewed and approved by the Approving Authority as detailed within Document Control.

11.3 Non-substantive, minor, or administrative changes may be made by the Policy Owner, or representative of the Policy Owner, as detailed within Document control.

12 Policies superseded by this policy

Not applicable.

13 Document control

VERSION	KEEPER	REVIEWED	APPROVING AUTHORITY	APPROVAL DATE	START DATE	NEXT REVIEW
1.0	Procurement	?	AS	27/09/2013		
2.0	Procurement	March 2014	AS	10/03/2014		
3.0	Procurement	June 2014	AS			
4.0	Procurement	April 2016	LJ	July 2016		
5.0	Procurement	October 2018	LJ	October 2018		
6.0	DTS	August 25				Sept 2027