Scope: University owned mobile devices	Effective Date: Feb 2024	Responsible Dept: ITS	Equality Analysis Undertaken:
Last Updated 2024	Next review date: Feb 2026	Associated links:	Policy Ref:MDP01

York St John Mobile Devices Policy

1. Introduction

This policy is applicable to all University staff.

The purpose of this policy is to set out the guidelines and standards which regulate the provision and use of University mobile phones, tablets, data cards and data equipment. In this policy, these will be referred to as a device or devices. Any York St John member of staff supplied with a University device is expected to abide by the terms and conditions outlined in this policy.

York St John University provides devices for staff to use in support of their business activities and work-related duties.

This policy must be read in conjunction with York St John University's Acceptable use of IT Services policy.

2. Principles

Requests for a University device must be submitted via a ticket via the ITS Support Portal https://www.yorksj.ac.uk/servicedesk. The request will be evaluated based on the eligibility requirements below.

3. Eligibility

The allocation of a University device will be subject to approval and to the member of staff meeting certain criteria. All requests for a device must be made through a member of the Executive or Senior Leadership team for approval.

Requests for a University device may be considered for:

- Staff who need to be contactable by the University whilst out of the office
- Staff designated as 'emergency contacts' for the University
- Staff whose roles frequently take them off-campus on University business
- Where there is a clear health and safety benefit to the staff member
- Where there is a clear benefit to the University of issuing a device

An ITS device loan service is available for staff to utilise for short term device usage.

Note: Staff working at home on an agile basis will be expected to use computer-based telephony e.g. MS Teams/Soft-phones and will not be automatically eligible for a mobile phone. The University does not provide mobile devices (such as dongles or phones) for connectivity in private homes. It is the responsibility of the individual to provide internet connectivity at home.

4. Mobile device usage

Mobile devices issued by the University are to be used primarily for work-related business and communications (call, SMS and data usage costs will be monitored and reports will be shared with relevant line managers).

Users may receive bills to reimburse the University for any excessive personal usage (the excessive use trigger will be reviewed annually and is currently set at a data usage of over 2GB per month).

All mobile devices **must be secured** with a password, PIN and/or biometric controls.

Use of, or subscription to, premium and/or interactive mobile services using a University device is prohibited. This includes, but is not limited to, the downloading or forwarding of ringtones, streaming of videos, television services and gaming apps. Users will be asked to reimburse the University for the use of unauthorised paid for services.

Devices should not be used overseas unless they have been specifically setup for use outside the UK and have been authorised for use abroad. Using a device abroad without the correct tariff can incur significant data roaming charges and any unauthorised costs associated with use abroad are the responsibility of the designated named user. A line manager can request for a device to be set up for use abroad via the ITS service desk, for either regular or infrequent travel.

Where available and secure to do so, devices should be connected to a Wi-Fi service to reduce the use of mobile data.

Physical SIM cards must not be removed from the supplied handset to another device. This may incur substantial cost for incorrect tariff usage and the University will seek full recompense for any additional charges incurred. Such action may also cause serious security breaches where the device carries confidential or sensitive University data.

The device is allocated for the sole use of the named member of staff only and must not be loaned or transferred to another user in any circumstance. An asset register will be kept by ITS linking the device to a specific individual and the designated named user will be deemed responsible for the device and its usage. Devices no longer required should be returned to the ITS to be repurposed.

The downloading and use of additional software, facilities, programs, or apps to the device is not permitted unless the software has already been approved by York St John University.

In addition:

1. All devices provided by the University, respective tariffs and licenses remain the property of university at all times
2. The device must be returned to ITS when a member of staff leaves the University, or there is a change in the job role which does not require the use of a device
3. The assigned user will be responsible for the security of the device, SIM card and any accessories.
4. Any loss or damage must be reported to ITS immediately
5. All device usage must comply with the IT Services Acceptable Use Policy Acceptable use of IT Services policy
6. Devices will be managed by ITS and the data usage and call usage will be monitored and shared with relevant line managers
7. The make and model of devices will be standardised (users can specify requirements but will not be able to specify specific makes and models)
8. Devices and associated mobile numbers will not be provided/transferred to individuals when leaving the University

5. Responsibilities

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

6. line managers' responsibilities

- Determining eligibility of staff and appropriate device(s) for their role
- Informing their staff members of their rights and obligations under this policy
- Ensuring only eligible staff have University issued devices
- Supporting ITS to manage usage costs
- Ensuring devices are returned when a member of staff moves or leaves their role within the University. Devices must be returned even if a new staff member is taking up the same role. Managers should return the existing device and request a new device for the new staff member. This is required to ensure compliance with data protection and security requirements)

7. User responsibilities

- Take reasonable care of University devices they receive
- Report lost, stolen and damaged devices to ITS
- Comply fully with legislation, this policy and related University policies
- Appropriately securing the device(s) and information held on it
- Deleting University information from the device when no longer required or sooner if required by the University to delete it

- When connecting to other devices ensuring that University data is not shared (e.g. a Bluetooth connection to a car may share all contact information held on the device)
- Updating the device (where possible) so that it has an up-to-date operating system
- University devices (including dongles) must not be used to provide connectivity for home working. The University is not responsible for providing internet connectivity in private homes.
- University mobile devices must not be used to take photographs of anyone without their consent
- Creation or transmission of material that infringes copyright is prohibited
- Devices must not be loaned or transferred to another member of staff.
- Users must return the device and SIM at the request of ITS for maintenance/renewal
- At the end of their life cycle, devices should be returned to ITS for compliant decommissioning

Users who are allocated a 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.

If you use devices such as laptops, smartphones and tablets, whether personal or University-owned, to connect to the University network and access University'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.**

8. Lost/stolen devices

- Any lost or stolen device must be reported immediately to ITS and your line manager
- A form will be issued requiring a full statement regarding the circumstances of any theft/loss will be required for data protection and compliance purposes
- ITS are required to report loss of corporate devices to the Governance team

9. ITS responsibilities

- Provide service support during normal business hours (Monday to Friday from 9am to5pm, excluding University closure days and bank holidays)
- ITS will manage the device contract and hardware warranty and renewal
- Monitor usage and provide appropriate reports on usage to relevant line managers

10. Privacy notes

- Devices are managed by the University's mobile device management platform, which means certain technical data is collected by our systems to allow the University to manage the mobile device estate
- Call, SMS and data usage is collected in the same way as with any mobile service provider, this is part of the service provision and is used for billing purposes
- Call and SMS content is not monitored but is captured and can only be accessed by following the ITS Controlled Systems Access policy

11. Related policies

- The Acceptable use of IT Services policy
- The ITS Controlled Systems Access policy