ABERYSTWYTH UNIVERSITY POLICY

Policy on Mobile phones issued by Information Services

Approving Body:	University Executive Group, Information Services Senior Management Group
Responsibilities:	Director of Information Services is@aber.ac.uk
Policy contact:	Data Protection and Copyright Manager Infocompliance@aber.ac.uk
Policy status:	January 2021 review
Review date:	January 2022

Table of Contents:

1. PURPOSE OF POLICY

This document sets out the University's Policy to regulate the issue and use of mobile phones, SIM card contracts and wireless devices (together termed 'mobile devices' for the purposes of this policy) issued to staff members and, in exceptional circumstances, others contributing to the business of the University, by the Department of Information Services.

2. APPLICABILITY/SCOPE/ELIGIBILITY

This Policy applies to all staff issued with mobile devices by Information Services and to any other individuals who may, from time to time, be issued with mobile devices in relation to the business of the University. All are referred to as 'users' throughout this document. The Policy covers:

- Eligibility for allocation of a University Mobile Phone.
- Mobile Usage
- User Responsibilities and Data Security
- Contract Obligations
- Managing Mobile phone contracts

3. RESPONSIBILITIES

3.1 Information Services Senior Management Group is responsible for the development, implementation, monitoring and review of this Policy.

3.2 Other levels of responsibility are detailed in the Policy section below

4. POLICY

4.1 Principles

4.1.1 The University will only provide a mobile phone/device if there is a clear business requirement specific to the individual role.

4.1.2 With the exception of members of the Executive Group, Institute Directors and Heads of Departments (who may request mobile devices for themselves), all requests for a mobile phone must be made by completing the mobile phone application form as found on the University Information Services website. This will require authorisation from an Institute Director or Head of Department who will only authorise the application once the business case has been assessed by them using the criteria listed in 4.1.3 below.

4.1.3 The eligibility of a user for allocation of a mobile device will be evaluated against one or more of the following criteria:

The user is required to be available outside business hours to assist with critical business functions of the University (e.g. responding to emergency situations, responding to ICT or building infrastructure problems)

The user is required to make regular calls when away from the office

The user is required to spend frequent or prolonged periods off campus

The user is required to spend frequent periods working alone

There is an identifiable and proportionate benefit to the University, such as Work allocation via a mobile phone app a SIM card in experimental systems or fire alarms etc.

4.1.4 Allocation of devices is determined on the basis of cost effectiveness and not personal choice.

4.1.5 Requests which are not appropriately authorised will not be processed.

4.1.6 Mobile devices ordered subsequent to such a request will normally need to be picked up in person by the intended user who should be able to present a current form of photo-identification.

4.1.7 In every case, devices should be collected within 7 days of the user being informed that the University has received that device.

4.1.8 Line Managers, senior staff and Information Services may view usage reports for monitoring compliance with this Policy.

4.1.9 Eligibility must be reassessed whenever a user/staff member transfers to a different post.

4.1.10 Mobile devices may be issued to a Department or section, rather than an individual, where there is a clear and legitimate need.

4.1.11 AU mobile devices will (wherever possible) be supplied with international and data roaming capability disabled. Users requiring these services will need to provide evidence of need and appropriate authority from their Director or Head of Department.

4.1.12 Upgrading to a new model of mobile device will also require authorisation if the existing model is still in working order.

4.1.13 Disposal of phones, all phones once a user has finished with them must be sent to Information Services to be placed back to factory settings or destroyed. This will ensure the wiping of any sensitive data that may be on the phone. If the department still require the phone for other users the phone will then be sent back for reuse following a data reset. Any phone that's old or broken and left for disposal, or been replaced by insurance swap outs may be used by information services as spare parts or repairs where appropriate.

4.2 Mobile Usage

4.2.1 Mobile equipment issued by the University should, primarily, be used for work-related business and communications.

4.2.2 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, videos and mobile-TV. Failure to comply may lead to disciplinary action being taken.

4.2.3 University mobile devices must not be used for the purposes or illegal transactions, harassment, obscene communications or any other activity which might breach another University policy.

4.2.4 The University does not permit the transfer of the University SIM card from the supplied handset to a personal device. This may incur substantial cost for incorrect tariff usage and the University will seek full recompense for any additional charges incurred. Such action might also cause serious security breaches where the device carries confidential or sensitive University data.

4.2.5 Users must not use a University mobile device whilst operating a motor vehicle. Any fines incurred as a result of traffic regulation breaches are the responsibility of the user involved.

4.2.6 Users may, on the payment of an extra charge (£10 per month – to be arranged via the Finance Department), utilise mobile devices for personal use. If this facility is made use of, it is on the condition that there is:

- No overseas use
- No use of premium rate phonelines
- No downloading of data in excess of the maximum limits set

If any of the above do become necessary, permission must be sought from the Director of Finance and a further charge may be levied.

4.2.7 User's must not install any un-signed applications to the device, this means only applications sourced via the Android or Apple "Play Store" app is allowed, unless directed by line management for specific departmental applications.

4.3 User Responsibilities

4.3.1 Users who are allocated a mobile device will be held responsible for the handset and all calls made and other charges incurred. It is therefore essential that devices are kept secure at all times and use by anyone other than the named individual is prohibited. Users should take all reasonable and practical precautions to keep the device safe from damage, loss or theft.

4.3.2 The handset/SIM PIN code or other security locking system should always be used. 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) must not be stored unsecured on a mobile device.

4.3.3 Handsets that are lost or stolen must be reported immediately to Information Services (2400 or 01970 622400 if outside the University) so that the handset can be deactivated. It is strongly recommended that users keep a separate note of their handset's IMEI number as this will need to be provided to the mobile provider to deactivate the handset, and also note their SIM number.

4.3.4 If a device is stolen, the user must report the theft to the police immediately and obtain a case number. Information Services should then be informed.

4.3.5 If a user loses more than three mobile devices within any one-year period, then the University reserves the right to refuse to issue any further devices to that individual.

4.3.6 Mobile devices remain the property of the University at all times and must be surrendered when a member of staff leaves employment or a user ceases to work on behalf of the University, or on demand by the head of department, or by Human Resources or Information Services. Users can purchase their mobile phone if desired and permitted by their department head or director. There is normally a fee for the value of the phone and this is negotiated by the department and the user.

4.3.7 Departments are responsible for ensuring that users issued with mobile devices have returned phones to the budget-holder or directly to Information Services

4.4 Contract Obligations, Budget-holder and other Responsibilities

4.4.1 No phone changes or re-allocations should be made unless approved by the departmental head, director or designated phone admin for the given department, further more information services must be informed for internal recharging and record keeping purposes.

4.4.2 Local or departmental budget-holders are responsible for:

- reviewing ongoing requirements for each mobile device funded from their budget
- reviewing the summary bills and addressing high call and data usage
- consulting Information Services regarding user charges

4.4.3 Porting of numbers to individuals for personal use will only be permissible via prior agreement from Director or Head of Department and from Information Services.

4.4.4 Devices that have reached the end of their working life must be disposed of legally as they fall under the WEEE regulations. All end-of-life devices must be returned to Information Services for disposal.

5. RELATED LEGISLATION/GUIDANCE

- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000 ("RIPA")
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)

6. RELATED POLICIES AND PROCEDURES

- AU E-mail Policy
- AU Data Protection Policy
- AU Data Security Policy

7. APPENDICES/FORM None

8. WELSH VERSION OF POLICY