University of Salford MANCHESTER

Mobile Devices Policy

(constitutes BYOD Policy *pro tem*)

Version Number: 2.0

Effective from 17 December 2015

Author: Senior Information Security Officer, Legal, Planning & Governance Directorate & ITS Technical Officer, IT Services

Document Control Information

Status and reason for development

Revised version of Mobile Devices Security Policy V1.0 incorporating organisational and strategic changes and expanding scope of policy to cover use of personally owned mobile devices. To be V2.0 when approved.

Revision History

Date	*Author*	*Summary of changes*	*Version*	*Authorised*
Apr 2015	Christa Price, Paul Turton, Jeremy Ford	Incorporated guidance on use of personally owned devices and Legal Services advice	V2.0	Info&Tech Mgt Group: 30/09/15. CIO: 18/11/15 Dir. LPG: 09/12/15
June 2011	Paul Turton, Christa Price	Policy approved and published	V1.0	Executive 13/06/2011

Policy Management and Responsibilities

Owner: This Policy is jointly owned by the Director of Legal, Planning & Governance, the CIO and the Associate Director of IT Operations who are responsible for issuing policy on access to and use of University information and use of IT devices.

Others with responsibilities: All staff must be aware of and comply with this policy.

Assessment	*Cross relevant assessments*	*Cross if not applicable*
Equality Analysis	X	
Legal	☐	X
Information Governance	X	☐
Academic Governance	☐	X

Consultation	*Cross relevant consultations (or N/A)*
Staff Trades Unions via HR	HR Policy Adviser Spring 2014 and Partnership Working Group Jan 2015.
Students via USSU	N/A
Any relevant external bodies	N/A
(please specify) ……..	

Authorised by: Information & Technology Management Group. Minor changes to the policy may be authorised by the Director LPG and the CIO on behalf of the ITMG.

Date authorised: 30/09/2015

Effective from: 17/12/2015

Review due: 3 years by December 2018

Document location: University Policy & Procedure Page

http://www.salford.ac.uk/about-us/corporate-information/governance/policies-and-procedures

Document dissemination and communications plan:

US Online and ITS / Finance will notify to users of University issued mobile devices (laptops, tablets and phones).

1.0 Purpose

This document specifies the University policy for the use, management and security of all Mobile Devices that may hold University information. This policy is an important part of the overarching University Information Framework. The Information Framework exists to ensure that all those who are authorised to, should be able to easily access all the information they need to fulfil their role.

2.0 Scope

This policy applies to all:

- University Issued Mobile Devices, *and*;
- Personally Owned Mobile Devices;

that are used to access University information, network or ICT facilities including, but not limited to, University information systems, staff Email, University managed storage (i.e. F drive and shared storage).

This policy applies to all staff and third parties (including but not limited to contractors, agency workers, associates and students) operating on behalf of the University or undertaking University functions and thereby accessing the above systems or who are provided with a University Issued Mobile Device. These will hereafter referred to as 'Users'.

This policy **only applies to students if** they are carrying out a function on behalf of the University i.e. similar to a staff member's function.

This policy applies to use of Mobile Devices for business purposes at all times, both during and outside office hours and whether or not Users are at their normal place of work.

This policy recognises that Personally Owned Mobile Devices are and will be used to access University information but makes no comment on the requirement or recommendation to do so nor does it mandate or recommend the use of personally Mobile Devices.

The University is under no obligation to modify its systems to allow Users to connect their Personally Owned Mobile Devices to them where such modification may be required.

Use of Personally Owned Mobile Devices to access and store University information, as well as a User's own personal content, is commonly known as 'bring your own device' or BYOD.

IT Services provides Service Desk support (**but not technician visits**) for Personally Owned Mobile Devices, where this is necessary to enable Users to access University information or University systems for business purposes.

2.1 Definitions

Mobile Devices include, but are not limited to:

- Laptop computers and netbooks
- Tablet devices
- Smartphones etc.
- Portable storage such as removable hard drives, USB memory sticks and data cards
- Portable audio visual equipment including data projectors, cameras etc

University issued Mobile Device means any **Mobile Device** that has been purchased, is owned or leased by the University (regardless of the source of funding).

Personally Owned Mobile Devices means any **Mobile Device** that is held personally by an individual in a private capacity.

Confidential information consists of information which, if disclosed or made publically available could damage commercial or financial interests, privacy, reputation or employability; could cause damage or distress to individuals; cause the University to not meet its legal obligations; or damage the University's reputation. The definition of Confidential includes any information which is either labelled as 'confidential' or, if not labelled 'confidential', would nevertheless be reasonably regarded as confidential. (See Information Security Policy listed in Related Documentation)

Collections of Mobile Devices: devices provided by the University on a short term basis as part of a loan / pool scheme and those provided as part of the University's meeting and teaching room resource.

University information means information relating to or connected with the University's business or affairs whether or not such information constitutes 'confidential' information.

2.2 Changes

This policy does not form part of the terms and conditions of employment of Users and the University may at its discretion review and amend this policy at any time. Provided that Users are notified of amendments (this can be through internal communications addressed to all staff), then they will be bound by the policy as amended.

3.0 Policy Statements

Protecting University information and facilities

3.1 The use of any Mobile Device to process and access University information creates risks including those relating to data protection, virus infection, copyright infringement, unintentional or unlawful compromise of data and even loss or theft of device and / or data. The risks are increased, and are also more difficult to manage, when using Personally Owned Mobile Devices.

3.2 The University, and its staff, is required to process, and is committed to processing, all personal data in accordance with the Data Protection Act 1998 regardless of the device used to access the information. University Users are required to keep University information and personal data secure (see Related Documentation). This applies equally to University information held on University systems and devices or accessed / held on Personally Owned Mobile Devices.

3.3 The University reserves the right to refuse to allow access to particular devices or software where it considers that there is a security or other risk to its information or ICT facilities.

3.4 The University is the owner of all University information and the contents of University systems together with everything which is created on, transmitted to, received on or printed from, or stored or recorded on each Mobile Device, in each case during the course of the University's business or otherwise on the University's behalf – irrespective of who owns that Mobile Device.

3.5 The University reserves the right to request access to inspect, or delete University information held on a Personally Owned Mobile Device to the extent permitted by law and for legitimate business purposes. Every effort will be made to ensure that the University does not access the private information of the individual. (See 4.0 Policy Enforcement).

3.6 Monitoring of University ICT activity logs (relating to Staff usage) whether using University Issued Mobile Devices or Personally Owned Mobile Devices, will be carried out in accordance with the ICT Acceptable Use Policy (See Related documentation).

3.7 Mobile Device Loan Schemes should incorporate the principles of this policy into their terms and conditions, making the person borrowing the device(s) aware of their responsibilities.

User Responsibilities

3.8 Mobile Device Users are responsible for;

- the security of University information and of the device on which the information is held (see Data Access and Storage section for provisions regarding Confidential Information)
- storing University information on the Mobile Device only for so long as necessary
- deleting University information from the Mobile Device when no longer required or sooner if required by the University to delete it
- ensuring (where possible) the device has up to date Operating system and anti-virus protection
- complying with this policy and the related policies (specified in Related Documentation).

Data Access and Storage

3.9 Use of any Personally Owned Mobile Device for business purposes is at the User's risk and the University is not liable for any losses, damages or liability arising out of such use, including but not limited to loss, corruption or misuse of any content or loss of access to or misuse of such Personally Owned Mobile Device, its software or its functionality.

3.10 When storing / processing confidential information on a mobile device, use of a University Issued Mobile Device (i.e. laptop or tablet) should always be seen as the preferred mechanism. Storage on Personally Owned Mobile Devices can put confidential information at risk of compromise and may be subject to varied technical standards, support, as well as access by third parties. Where a Personally Owned Mobile Device is chosen over a University issued one, it should be authorised in writing by the relevant Head of Department or Head of School.

3.11 Confidential information should be stored within and accessed from University information systems and University managed storage to ensure security of and appropriate secure access to the information.

3.12 Confidential information should not be stored or transferred to a cloud computing service (such as personal skydrive or dropbox accounts) **unless** it is under a University negotiated contract. The contract should address the issues of confidentiality, integrity and availability of the information **and** should be approved by IT Services and Legal, Planning & Governance. (See the Information Security Policy in the Related Documentation).

3.13 Only store the minimum amount of information necessary (to carry out any required task) on a mobile device. A temporary cache may be held on the device, therefore any Confidential information should be deleted from the device as soon as the information is no longer required.

3.14 Remote access i.e. off site or via wireless for Users is limited to the services available via the Portal, ActiveSynch or Blackboard VLE.

Device and physical security

3.15 Mobile Devices accessing University information must have a strong (4 or more alphanumeric characters/ pattern) password / passcode / PIN enabled to reduce opportunity for unauthorised access. Passwords / passcodes / PINs must be kept secure. The device should be set to automatically lock if inactive for 5 minutes or less, or locked manually using Ctrl, Alt & Delete keys. (See Related Documentation for further advice).

3.16 Mobile Devices used to regularly access/store Confidential information should be subject to additional protection measures (such as encryption) to reduce opportunities for loss or compromise of the information.

Technical security: From 1 August 2014, IT Services ensures any new purchases of University laptops will be hardware encrypted as standard. New purchases of portable storage devices (i.e.

hard drives or USB memory sticks) must be obtained via IT Services to ensure they are hardware encrypted.

3.17 Mobile Devices should, where possible, have operating system and anti-virus updates enabled. "Jailbroken" or "rooted" devices or those mobile devices which have otherwise circumvented the installed operating system security requirements (making them vulnerable to compromise) are not permitted to connect to the University ICT facilities.

3.18 University Issued Mobile Devices are configured to standard security and other settings and tariffs before delivery to the User. Any changes required to these settings and tariffs must be requested via the ITS Service Desk for authorisation by IT Services and IT Purchasing respectively.

3.19 **Physical security:** University Issued Mobile Devices must not be left unsecured whether on or off University premises. When unattended the device must be locked (password / passcode / PIN protected) and the mobile device should be secured with a recommended 2 barriers i.e. limited access building or office **and** where possible a locked cupboard. There should be **limited and controlled access** to the cupboard keys, not left in the cupboard or on a shelf. The University ID card provides auditable access control and will be more effective than duplicate (or more) copies of office keys (contact Maxwell Security team for physical security advice).

Users must take responsibility for a mobile device and not leave it unattended in:

- busy public areas
- when travelling *or*
- a car, including in its boot.

3.20 IT Services staff will ensure University issued Mobile Devices are not left unattended at any point in the delivery or installation process. This will include signed receipt of collection/delivery by the User.

When an employee leaves or changes mobile device

3.21 **University Issued Mobile Devices** must be uniquely identified, security marked (where possible), and linked to a User. Issue / loan records will be kept accurate and up to date.

a) The devices are University property and as such must be returned to IT Services upon change of User or termination of employment. They must not be sold, given away or otherwise be disposed of by the User.

b) IT Services will manage the re-image before re-issue to another User (or secure erasure when disposing of devices at end of life).

c) If devices are not returned (after a reminder process) the matter will be passed to the Head of School / Division as a disciplinary matter. The matter may also be passed to the Police for consideration of further action or for recovery via civil litigation.

3.22 **For Personally Owned Mobile Devices**, employees must delete all University information from their device (on termination of their employment or, if the Personally Owned Mobile Device is repaired, exchanged, sold, given away or otherwise disposed of) and may be required to provide a written undertaking that this will be done. Without relieving employees of their obligation to delete all University information, the University's rights under paragraph 3.5 above apply, including after termination of employment.

Costs associated with Mobile Devices

3.23 In line with the ICT Acceptable Use Policy, University Issued Mobile Devices are provided for University business use and some limited personal use is allowed. However this should be in agreement with the owning School or Professional Service and arrangements made locally to repay costs of any personal use.

3.24 Itemised bills for University issued phones will be checked by the local Finance Manager. Where arrangements have not been made to repay costs of personal use or a User cannot justify unauthorised or excessive costs it is the discretion of the Dean of School / Professional Service to initiate disciplinary action in line with the Staff Disciplinary Policy.

3.25 The use of mobile devices overseas can lead to potentially significant costs, for example through data roaming, as well as risks to the device. Users must obtain approval from their Dean of School / Professional Service for overseas travel with a University Issued Mobile Device. It is the User's responsibility to contact the ITS Service Desk before travel to arrange for the correct package to be applied to their phone and also to receive and implement operational instructions on applying settings to ensure no unnecessary and avoidable costs are incurred. As per Finance rules, the costs for a single international trip will be paid by the University up to a maximum of £50.00 (NOTE: that this should not be the claim for every international trip) regardless of whether the mobile device is University issued or personally owned (local arrangement). Costs over and above this for University devices for an international visit will be reclaimed from the individual.

3.26 There is no University policy on the re-imbursement of costs or data plans for Personally Owned Mobile Devices. Any such arrangement should be determined locally.

Reporting loss or theft

3.27 In the event of loss or theft of any Mobile Device irrespective of whether it is a University Issued Mobile Device or a Personally Owned Mobile Device (used to access University information, network or ICT facilities), the User must act promptly to **minimise the risk of compromise to University information** by immediately;

- changing their university network log-in password and notifying ITS Service Desk of incident circumstances. A lost / stolen proforma must be completed and returned to IT Services (See Related Documentation)
- changing any other passwords that may have been used on the device (e.g. banking)
- reporting **theft** of device to the Police (and Estates Security, whether on **or** off Campus)
- reporting loss or theft of mobile phone to the mobile network carrier directly.

3.28 Appropriate steps will be taken to ensure that University information on or accessible from the Mobile Device is secured, including remote wiping of the Mobile Device. The remote wipe will destroy all University data on the Mobile Device. Although it is not intended to wipe other data that is personal in nature (such as photographs or personal files or emails), it may not be possible to distinguish such information from University data in all circumstances. Users should, therefore, regularly backup all personal data stored on the Mobile Device.

4.0 Policy Enforcement and Sanctions

4.1 Reports of loss or theft may be forwarded to the relevant Dean of School / Director of Professional Service to investigate in accordance with appropriate legislation and University Policy. Investigations will follow investigation procedures as outlined in the ICT AUP and Forensic Readiness Policy (See Related Documentation). Sanctions for non-compliance with this policy may include;

- Investigation into circumstances of the loss or theft of mobile device
- Revocation of access to University systems
- Initiation of disciplinary action in accordance with the Staff Disciplinary Policy in the case of employees, termination of the agreement in the case of a contractor or agency worker, or Student Disciplinary Policy in the case of students

- Removal of User rights to request a University Issued Mobile Device
- Removal of University information from the User's Mobile Device
- Cost of replacing lost/stolen equipment charged to relevant School/Division
- Referral for non-return of mobile device for police attention or pursuance of civil recovery.

4.2 Users must co-operate with the University to enable access, inspection and other authorised activities in relation to their Mobile Devices used to access University information. This may involve providing the University with access to the Mobile Device.

4.3 Any actual or suspected misuse of Mobile Devices or breach of this policy should be reported to the ITSERT (via IT Services Service Desk)

5.0 Related Documentation

Policies: Mobile Device Users should also be aware of and comply with the related University policy listed below:

University Policy & Procedure pages: http://www.salford.ac.uk/about-us/corporate-information/governance/policies-and-procedures

- IT Procurement Policy
- ICT Acceptable Use Policy
- Forensic Readiness Policy (draft)
- Data Protection Policy
- Information Security Policy
- Network Security and Connection Policy
- Student Disciplinary Policy

HR Document Finder: http://www.hr.salford.ac.uk/policies-procedures/

- Staff Disciplinary Policy
- Tele Home working Policy

ITS Service Desk 'top forms' list http://www.its.salford.ac.uk/servicedesk/

- Lost/Stolen proforma / Incident Reporting Form

Guidance

For guidance:

- Head of Security, Estates & Property Services can provide guidance on physical security measures/risk assessment.
- Information security and management advice from Information Governance, Legal Planning & Governance Directorate.
- Digital Skills online guidance http://www.salford.ac.uk/staff-development

6.0 Appendices

Appendix 1: Mobile Devices Policy – User Agreement.

Appendix 1: Mobile Devices Policy Agreement

Please sign the below agreement and return the signed page to University of Salford IT Purchasing, IT Services, Humphrey Booth or email ITS-purchasing@salford.ac.uk . Please retain a copy of the policy for your own reference.

I confirm that I have read, understood and agree to abide by the attached Mobile Devices Policy V2.0 specifying my responsibilities when accessing or storing University information on a University Issued Mobile Device. I will keep the copy of the Mobile Devices Policy for my personal reference.

Name (in capitals):	
Role:	School/Professional Service:
Signature:	Date: