# Mobile Devices Security Policy

## 1.0 Policy Administration

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Mobile Devices Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Category</td>
<td>Policy</td>
</tr>
<tr>
<td>Policy ref.</td>
<td>Unique ref no. Issued by GSU (P0001)</td>
</tr>
<tr>
<td>Version Number</td>
<td>V1.0</td>
</tr>
<tr>
<td>Status</td>
<td>New</td>
</tr>
<tr>
<td>Reason for development</td>
<td>Lack of existing University wide policy</td>
</tr>
<tr>
<td>Scope</td>
<td>This Policy applies to: All Staff and students issued with a University purchased / leased mobile device</td>
</tr>
</tbody>
</table>

### Executive Summary

The policy specifies the University and individual user responsibilities for securing, managing and using University owned and leased mobile devices. This includes laptops, pda’s, mobile and smart phones. Users issued with such mobile devices must explicitly comply with and sign the User Agreement at Appendix 1. Appendix 2 details a new single line of reporting for lost or stolen devices replacing the previous multiple and sometimes inconsistent reporting approach in the past.

Managing the issue, use and return of these devices is an essential part of the University non-pay savings.

### Author/developer

| Author/developer | Senior Information Security Officer | Owner | Head of Governance Services Unit and Director IT Services. Approval May 2011. |

### Assessment

- Information Governance - completed
- Equality Impact Assessment - completed
- Academic Regulation – not applicable
- Legal – not applicable

### Consultation

- Not applicable

### Authorised by (Board)

| Executive Committee | Date: 13/06/2011 |

### Effective from

20/06/2011

### Review due

2 years – by June 2013.

### Document location

IT Services webpages for transfer to new University policy pages (Autumn 2011)

### Document Dissemination/Communication Plan

- US online briefing to all staff
- ITS Finance manager to brief all College and PAS Finance staff
- ITS briefing to all ITS and University Technicians
- Issue of User Agreement to all mobile device users for signature and return. Completion of user agreement will be a precondition to receipt of a mobile device for phased replacement or new
2.0 Purpose

This policy provides a minimum specification for the security, management and use of University owned and leased mobile devices.

3.0 Scope

The policy applies to all staff, students and associates within the University of Salford. The policy relates to University owned or leased mobile devices including (but not limited to):

- Laptops
- Mobile phones, PDAs and smart phones
- Portable audio visual equipment including data projectors, cameras etc
- Meeting and teaching room IT equipment
- Collections of mobile devices used for loan or pool schemes.

This policy does not cover the purchasing process, taxable benefits issues, or health and safety aspects of mobile devices. It does not cover data storage media or the use of privately owned mobile devices to connect to University ICT facilities (see Related Policies).

4.0 Definitions

Confidential data in this policy is defined as information relating to living individuals or commercially sensitive information, which, if compromised, may:

- cause damage or distress to individuals by compromising their right to confidentiality and privacy (Data Protection Act 1998);
- damage reputation of University in the sector;
- cause University to not meet its legal obligations; or
- compromise network security.

Mobile worker in this policy is defined as a staff member for whom issue of a University laptop and / or mobile phone is justified and relevant to his / her work.

Laptop issue is justified for staff members who are:

- Required to work away from their primary workspace / office desk, either across campus (where existing IT facilities are not available) or offsite and require computing facilities to undertake their role.
- Expected to work out of core hours e.g. from home evenings and weekend, as defined in their job description and have a need for access to files and work applications.

Mobile phone / smart phone issue is justified for staff members who are:
• Required to be contacted out of core hours
• Required to maintain frequent and immediate business communications access when away from the office i.e. calls, email, calendar.

Collections of mobile devices in this policy are defined as technician’s stores, pool laptops, audio visual equipment or laptop loans schemes.

5.0 Governance and Management

This policy is issued jointly by the Head of Governance Services Unit and the Director of IT Services (ITS) who, as Chief Information Officer of the University has the responsibility for (and the authority to delegate responsibility for);

• Issuing policies and procedures for the University ICT facilities and services
• Managing and protecting the ICT facilities and services
• Investigating breaches of this policy and applying sanctions directly or referring for disciplinary action where relevant.

IT Services manages the University mobile phone contract, however the allocation and management of mobile phone usage is the responsibility of the relevant College PVC Dean or Professional Administrative Service (PAS) Director. ITS Purchasing will issue guidance on performance Indicators in this area.

6.0 Policy statements

Secure storage and asset database

6.1 The nature of the University estate is to be open and accessible to staff and students. Unrestricted access poses risks to our data and assets therefore all protection measures should be appropriate to the risk to the asset and the consequences of a compromise. All mobile devices should be secured, when unattended, with a minimum of 2 barriers i.e. building controls and locked office or locked drawers/cabinet.

6.2 Collections of mobile devices (see Definitions) require more stringent physical security measures than a single item issued to a user. Physical security risk assessment should be requested from the Security Team, Estates & Property Services.

6.3 IT equipment must not be left unattended at any point in the delivery or installation process. The process will include signed receipt of delivery to the user (Appendix 1).

6.4 All University laptops will be uniquely identified and registered in the University’s IT asset database. All new laptops will be asset tagged, security marked (where possible) and recorded in the University asset database as part of the installation process prior to delivery to user.

6.5 Accurate records will be held for any collections of mobile devices used for pool or loan schemes. Guidance on loan scheme documentation is available from the Senior Information Security Officer, Governance Services Unit.

6.6 Staff members are responsible for the security of the mobile device issued to them (including pool / loan scheme managers) and must not leave it unattended or insecure (Appendix 1). This includes making arrangements for secure storage with the support of his/her line manager.
6.7 University data should be stored within the University network drives or information systems. Mobile devices or external 3rd party facilities must not be used as permanent storage for electronic information belonging to the University (See Related Policies).

6.8 Laptops for users dealing with confidential data (see Definitions) should be subject to additional care and protection to prevent unlawful loss or compromise of the data.

Mobile Phones
The following requirements relate to mobile phones and are in addition to those listed in the ICT Acceptable Use Policy.

6.9 Mobile devices are configured to standard builds and tariff bands before delivery to the user. Any changes required to these settings e.g. changing roaming rates must first be put in writing to the ITS Service Desk for assessment and authorisation by ITS Purchasing.

6.10 Issued mobile phones are for University business use. Usage should be reasonable and justified in relation to work. Personal usage is permitted however, this should be reasonable, not excessive and arrangements should be made locally to repay costs of personal use.

6.11 It is the responsibility of the relevant College Accountant / PAS Head of Finance to check itemised bills, ensuring that call volumes and costs are appropriate and not excessive (for work purposes as well as any personal use) within his / her College or Division. Where a user cannot justify call usage and costs on a repeated basis, it is the discretion of the PVC Dean / PAS Director to initiate disciplinary action in line with the Staff Disciplinary Policy.

University property
6.12 University purchased and leased mobile devices are University property (regardless of the source of funding). They are not a user’s personal property nor are they available for individual resale or remuneration.

6.13 All University purchased and issued laptops must be returned to IT Services upon termination of employment, research contract or work agreement. If devices are not returned, after a reminder process, the matter will be passed to the Police for their consideration to take further action or for recovery via civil litigation.

6.14 ITS will securely erase data on mobile devices and reformat the device before re-issue to another University user. The device will also be securely erased when disposed of at the end of its lifecycle.

Reporting loss or theft of device
6.15 In the event of loss or theft of a mobile device the user should follow the process in Appendix 2 and immediately report thefts to the Police, then inform the ITS Service Desk. In relation to theft or loss of a mobile phone the user should also notify the Mobile provider directly.

7.0 Policy Enforcement and Sanctions

Failure to comply with this policy will be investigated thoroughly in accordance with appropriate legislation and the University Disciplinary Policies. Sanctions for violations of the policy may include;

- Cost of replacing lost/stolen equipment charged to relevant School / PAS
- Removal of rights as a mobile worker
- Referral of mobile device non-return for police attention or pursuance of civil litigation
- Initiation of Disciplinary Policy

8.0 Related Documentation

- IT Procurement Policy
- ICT Acceptable Use Policy
- Network Connection & Security Policy
- Data Storage Security Policy (in draft)

Controls addressed in this policy from ISO/IEC27001:2005 Information Security Management Systems - Requirements

<table>
<thead>
<tr>
<th>7.1.1 Inventory of assets</th>
<th>9.2.5 Security of equipment off premises</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1.2 Ownership of assets</td>
<td>9.2.6 Secure disposal</td>
</tr>
<tr>
<td>8.3.2 Return of assets</td>
<td>9.2.7 Removal of property</td>
</tr>
<tr>
<td>9.1.1 Physical security perimeter</td>
<td>10.7.1 Management of removable media</td>
</tr>
<tr>
<td>9.1.2 Physical entry controls</td>
<td>10.7.2 Disposal of media</td>
</tr>
<tr>
<td>9.1.6 Delivery and loading areas</td>
<td>11.3.2 Unattended user equipment</td>
</tr>
</tbody>
</table>

9.0 Appendices

Appendix 1: Mobile Devices User Agreement

Appendix 2: Reporting procedure for lost / stolen mobile devices
Mobile Devices Security Policy User Agreement

You are responsible for the security and use of the mobile device issued to you and you are expected to take the reasonable steps as listed below to protect the device and its data from theft, damage, misuse or confidentiality breaches. This responsibility applies at all times irrespective of whether at work or off-site. All mobile device users must sign to confirm acknowledgement of and compliance with these conditions.

Loan schemes and pool devices will also comply with the principles of this Agreement and those staff responsible for such schemes will sign the agreement for their pool / loan scheme devices and make users aware of their responsibilities.

1. Secure the device on University premises when unattended using a minimum of 2 barriers e.g. building controls and locked office or locked drawers/cabinet or a laptop security cable. Contact your line manager if such options are not available.

2. Do not leave a mobile device (your own or a pool device) unattended in insecure areas such as University meeting rooms or other public access areas. When off campus and the device is not in use, ensure that it is stored securely out of sight. Do not leave the device in your car boot for any period of time, especially overnight. Any devices left on display or unattended will be vulnerable to theft and / or data compromise.

3. Be aware of the potential for opportunistic or targeted theft of mobile devices in busy public places including airports, public transport or hotel lobbies. Keep it with you at all times especially at airport scanners and during travel. Be aware of shoulder surfing when working on confidential material. Do not leave your removable media in an unattended computer.

4. Do not take the mobile device overseas without:
   a) business trip authorisation of the Head of School / PAS Director and;
   b) tariff check from ITS Purchasing (via ITS Service Desk) to ensure the correct tariff band has been applied.

5. Do not tamper with or make changes to the standard settings and builds without written authorisation from ITS (via ITS Service Desk)

6. Ensure PIN / Password protection is enabled on the device as a minimum.

7. Connect the laptop to the network regularly to update the operating system and University anti-virus protection – the laptop is only as secure as the last time it was updated. Staff and visitors must take care to virus check any removable media to reduce the risk of introducing viruses or malware to the network.

8. University data should be stored within the University network drives or information systems. Mobile devices or external 3rd party facilities must not be used as permanent storage for electronic information belonging to the University.

9. Users dealing with confidential data (see Definitions) should take additional care to protect it from unlawful loss or compromise.

10. Do not allow family members or friends to use your University issued mobile device.

11. Do not download and install shareware/freeware/games on the mobile device. Approved software should only be installed after advice from ITS Service Desk or by an authorised University IT technician.

12. Do not use hand held mobile devices whilst driving (in line with UK and European legislation)

13. Do not incur excessive and unnecessary call costs to the University by repeatedly:
   1. selecting incorrect tariff bands
   2. failing to configure most cost effective connection method for data/email active synchronisation
3. failing to make adequate and ITS authorised arrangements (in advance) for overseas travel regarding network coverage and costs
4. failing to repay personal use costs where required

14. Do not use the device for offensive, inappropriate or excessive personal use including (but not limited to); premium rate chat lines, gaming, pornography or streaming movies (see ICT Acceptable Use Policy for full details).

15. Where mobile devices are issued as part of your role you are required to carry the device at all reasonably appropriate times and ensure the device is charged and available for use. The device should be appropriately handled, kept in good working order using an appropriate carry case (considering crime prevention advice). In the event of any technical problems with your laptop contact the ITS Service Desk. Contact the phone provider directly.

16. Delete data from a pool / loan scheme device before returning it.

17. Pool/ loan scheme managers should carry out a regular check of mobile devices against their inventory and should notify any changes in role pool / loan scheme manager to the ITS Service Desk.

18. Return the mobile device to IT Services at the end of your work or research contract. It is University purchased property not personal property. If device(s) is / are not returned, the matter will be passed to the police for their consideration or for recovery via civil litigation. The device will be re-formatted before re-distribution to another University user.

19. Notify the ITS Service Desk of any change of role, office location, School or PAS.

20. In the event of loss or theft of a mobile device you should follow the process in Appendix 2 and immediately report thefts to the Greater Manchester Police on 0161 8725050 (obtaining the Crime Reference number), then inform the ITS Service Desk on 0161 2952444. If your University issued mobile phone is lost or stolen, please also notify the Mobile provider directly in addition to the above reports.

Instructions: Sign and return this form by internal post to; IT Purchasing Team, IT Services, 4th Floor Humphrey Booth Building as soon as possible. Keep a personal copy for your reference.

Statement of Compliance: I understand and agree to comply with the Mobile Devices Security Policy and User Agreement for any mobile device issued to me.

<table>
<thead>
<tr>
<th>Name:</th>
<th>Username:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signature:</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Reporting procedure for lost / stolen mobile devices

1. User reports lost / stolen device to ITS Service Desk 0161 2952444
2. User reports stolen device to Police (obtain Crime Ref) 0161 8725050

SD assigns case to ITS Purchasing

- ITS Purchasing updates asset register
- ITS Purchasing email case info to:
  - Estates Security
  - Finance Division
  - School/PAS Finance Mger
  - ITSERT

User sends incident proforma to ITS Purchasing

- ITS Purchasing progresses purchase

SD assigns task to Compliance for investigation

- SD creates case incl. Crime Ref No. Change user’s passwords.

SD assigns case to ITS Purchasing

- SD Case info required for lost/stolen mobile device:
  - Crime Ref No.
  - Date stolen / last seen
  - Location stolen from e.g. Building & room
  - What happened

Force a user password change

End