Information Systems

Mobile Device Policy

Purpose of this Document

This document describes the policy for the management of mobile devices.

This document will be reviewed every 12 months

Author:	Matt Mason
Version:	1.1
Date:	8th May 2012

NOTTINGHAM TRENT UNIVERSITY

REVIEW/APPROVAL HISTORY FOR THIS DOCUMENT:

Organisation	Action	Date
IS Management Team	Provide overall direction for content	April 2011
NTU Senior Management Team	Approve document for publication	June 2011

DOCUMENT CONTROL:

Version	Author	Date	Version details	Reviewer	Date
0.1	Chris Toseland	16/03/11	First Draft	Richard Eade	16/03/11
1.0	Chris Toseland	15/04/11	First Draft	Richard Eade	15/04/11
1.1	Matt Mason	08/05/12	Annual Revision	Peter Nicholson	09/05/12

CONTENTS

Executive Summary

The University has an obligation as a publicly funded entity to ensure that it ensures value for money. As mobile devices usually carry a cost premium Information Systems shall carry out a needs based assessment on requests for this type of equipment.

This document describes the policy for the provision and management of mobile devices.

This policy applies to all Nottingham Trent University staff and enrolled students.

Governance

It shall be recognised that the management and ownership of all University owned IT assets is the responsibility of Information Systems, as devolved by the University Senior Management Team.

IT asset management is regulated by the Service Transition Manager and the Computer Use Regulations for Nottingham Trent University.

Definitions

User – A member of staff or enrolled student of Nottingham Trent University or an authorised 3rd party

IT Asset – A physical item of IT equipment such as but not limited to; workstations, laptops, printers, monitors and mobile communications devices.

Mobile Device – A portable item of IT equipment such as but not limited to; laptop/notebook, PDA, iPad, tablet, portable storage devices (disks/mp3 players) and mobile communications devices.

CMDB – Configuration Management Database. Information Systems 'register' of IT assets.

WEEE directive - Waste Electrical and Electronic Equipment Directive, a government directive concerning the safe disposal of electrical equipment.

Strong Password – A password that contains a combination of numbers, symbols and a mix of upper and lowercase characters.

POLICY

1. General

1.1 Users of University-owned IT assets will be subject to the NTU Computer Use Regulations.

2. Request and Authorisation

2.1. All requests for mobile devices shall be submitted to the IS Service Desk in the first instance.

2.1.1. If requests for mobile devices cannot be serviced from existing stocks the user will be provided with, and be required to fully complete an IT Purchase Request Form. The request form must include a full description of the business need.

2.2. Authorisation for the allocation of mobile devices:

2.2.1. Shall be given by the relevant budget holder or a duly appointed nominee.
2.2.2. In the case of a request falling under 2.1.1 authorisation shall be sought as per the IT Purchase Request Form process.

3. Delivery and Recording

3.1. It is a University requirement that Information Systems hold an accurate record of IT assets, to this end:

3.1.1. On arrival all mobile devices must have a uniquely numbered asset tag affixed.
3.1.2. The IT asset must be recorded in the CMDB. The recorded information must include as a minimum; asset tag, manufacturer, part number, serial number, MAC address (where appropriate), category, subcategory, physical location and delivery date.

4. Deployment

4.1. Where laptops/notebooks are provided the User will be provided with a docking station, keyboard, mouse and monitor this will then become their normal workstation. The existing desktop computer will be removed for disposal or redeployment.

5. Security

5.1. Data loss is a major risk to the University due to the sensitive nature of information held whether it be research or student data. A failure to implement adequate controls over information may leave the university open to significant reputational risk, as well as penalties from the Information Commissioner, to this end:

5.1.1. University owned Laptops/notebooks must have their data encrypted and any local accounts must have a strong password.
5.1.2. Users must take all reasonable precautions to ensure the physical security of mobile devices. Such measures may include the use of security cables or putting devices into a secure location such as locking in a desk drawer or cupboard within an office when it is unattended.
5.1.3. In the case of theft a crime number must be obtained from the Police and **Information Systems should be notified immediately**.
5.1.4. In the case of loss Information Systems should be notified immediately.

5.1.5. Information Systems will hold equipment for disposal in a secure storage area until such time that it is collected by a University approved contractor who guarantee physical destruction of the data.

6. Auditing and Periodic Reviews

6.1. Information Systems will deploy such automated auditing and deployment tools as are required to assist in the management of the IT assets.

6.2. Staff issued with laptops or other mobile devices will return them to Information Systems when requested to enable periodic audits and health checks to be performed.

6.3. Information Systems will audit the existence and physical location of IT assets on an ongoing basis and update the CMDB.

6.4. Information Systems shall review IT asset usage quarterly and where there is clear evidence of underutilisation may chose to exercise the option to redeploy IT assets to areas of greater business need.

7. Returned and Recovered Equipment

7.1. Equipment that is returned to, or recovered by Information Systems will be placed in a secure storage area and where appropriate processed as per the IT Asset Management policy.

8. Disposal, Theft and Loss

8.1. In order to comply with the WEEE directives all IT assets are classified as hazardous waste once they are deemed to have reached the end of their useful life and will be treated as such.

8.2. Information Systems does not allow IT assets to be donated, gifted, sold or otherwise removed from University premises. All IT equipment will be disposed of by a university appointed WEEE waste handler. Breaches of this policy may result in disciplinary action.

8.3. IT assets are owned by the University and managed by Information Systems, decisions on their disposal or permanent removal from the ownership of the University is solely the domain of Information Systems. Any IT assets found to have been permanently removed from the University without Information Systems prior approval will be investigated and may result in disciplinary action being taken.

8.4. If any IT equipment is lost or stolen, it MUST be reported to the Service Desk at the first opportunity in order that this is recorded and to take any remedial action to prevent loss of data or to protect users.

Other Supporting Documents

IT Purchase Request Form – Is provided to the User by their Business Relationship Manager should IT assets be unavailable from current stocks.

NTU Computer Use Regulations – Regulations accepted by users when granted access to the University Computer Network.

Mobile Phone Policy - details the policies for providing mobile phones and mobile services.

Responsible Manager

The Service Transition Manager is responsible for the development, compliance monitoring and review of this policy and any related procedures.

Implementation Officer

The Information Security & Audit Manager is responsible for the dissemination and implementation of this policy throughout IS.