University for the Creative Arts

Mobile Working and Remote Access Policy

Version 1.0
Author: Marion Wilkes
Date: 20 July 2009

Document History

Version History

1.0	20 July 2009	Approved for publication by the IS Board after E&FC approval in June 2009

Purpose and Scope

1. The purpose of this policy is to maintain the security of the University's information assets when they are transferred to mobile devices or accessed from locations outside the University's campuses. It applies to the University's staff.

2. Mobile devices, for the purposes of interpreting this policy, are defined as being any portable, hand-held computing and/or communications devices that are currently available or may be in the future. They include, but are not limited to, Laptop computers, Personal Digital Assistants (PDAs), Blackberries, mobile phones, USBs and cameras; these devices need not be owned by the University. The University's Information Handling Policy sets out the minimum standards that must be adhered to when handling sensitive information. Those standards apply equally when handling sensitive information on mobile devices or when such data is accessed remotely.

Authorisation

3. Staff may not copy classified data (see Information Handling Policy for a definition of 'classified' data) to a mobile device unless they have been authorised to do so by the information owner. Where appropriate, such authority may be given on an ongoing basis and as part of the process of setting user permissions put in place by information owners.

4. Remote access to the University's information systems and information assets must be authorised by the owners of those systems and assets. Such owners should undertake a risk assessment based on the criticality of the information assets being used and the appropriateness of the proposed location.

Avoiding theft and accidental loss of mobile devices

5. Mobile devices are often high value items that are frequently the subject of opportunistic theft. In these circumstances it is not the data held on these devices that is targeted by the thief and indeed in many cases it will be erased, however the loss of the data could be a much more serious consequence of the theft than the loss in monitory value of the device and it could lead to legal action being taken against the University or the individual under the Data Protection Act, should sensitive data be disclosed.

6. Users must ensure that unattended equipment has appropriate security protection and every reasonable precaution must be taken to ensure that unauthorised persons do not gain access to it. The following security precautions must be followed:

    - Never leave mobile devices unattended in an open or unlocked office
    - When working in an open office environment always secure laptops to a desk or large piece of furniture with a 'Kensington Lock'
    - Lock Blackberries, PDAs and mobile phones in desk drawers or cupboards when not being used or carried with you
    - Do not leave mobile devices visible in parked or unattended cars
    - Portable computers should be carried as hand luggage when travelling.
    - CD, DVDs and portable storage media must never be dispatched as unregistered post. If they contain classified data, such data should be encrypted and password protected.

Data Security on mobile devices

7. Staff who have been authorised to store classified data must encrypt and password protect the stored data.

8. All PDA devices should be password protected. Content Protection should be enabled on Blackberries to encrypt locally stored data. University-owned and University-supported PDAs should be configured to make use of remotely enforced security policies available via Microsoft Exchange and Blackberry Enterprise Server, which can provide and local and remote device wiping in the event of repeated failed login attempts. Consult the IT Helpdesk for advice.

9. The following measures should be implemented on portable computers:

    - The use of time out software protection.
    - Screensavers that require the use of a password to continue.
    - The use of a keyboard lock

10. Staff using portable or other computing devices at home that are connected to a network must install appropriate firewall and anti-intrusion software. Consult the University IT Helpdesk for advice on the best software and security settings to use.

11. Passwords must not be stored within email clients, browsers or login scripts on a mobile device.

12. Staff may not process classified data, whether in electronic or in hard copy, in public places e.g. on public transport.

13. Utmost care must be used when transporting files on portable media to ensure that valid files are not overwritten or incorrect or out of date information is not imported.

14. Avoid storing any data that is no longer needed; destroy CDs and DVDs by cutting with scissors and delete data stored on portable drives.

15. Mobile devices that contain or access classified information, or have been used to access classified information in the past, must be processed to ensure all data is permanently removed in a manner that prevents recovery before their disposal or transfer to another user. Deleting files and/or reformatting a device is insufficient to prevent recovery of data.

16. All emails containing classified data or sensitive information must be deleted from laptops and Blackberries once they have been read.

Data security and remote access to University systems

17. Remote access to the University's systems should always be protected through the use of MOTP (Mobile One-Time Password), which should be set up in conjunction with the IT Helpdesk.

18. Classified data should only be accessed from equipment in secure locations; files must never be printed on a networked printer that does not have adequate protection or security.

19. Staff accessing University systems remotely are responsible for:

    - Making adequate backups, where appropriate, onto suitable media
    - Virus checking all data which is sent / transferred to the University from the home using the software, and adhering to procedures provided by the University.
    - Preventing access to any University systems by other third parties in line with licence terms.

1.