Information Services

Regulations for use of Mobile Devices Owned by the University and Connected to the University of Kent Network

Scope

1. These regulations apply to: all students registered at the University, all members of staff employed by the University, all visitors and others using a mobile device owned by the University. All are required to adhere to regulations guidelines to ensure procedures are followed so that the risk of confidential and sensitive data being compromised is kept to a minimum.

Definitions

2. A mobile device is portable and to which data can be transferred, it is not limited to but includes laptop/netbooks, smart phones (like an Apple iPhone, an android phone), iPod Touch, tablets (like an Apple iPad and the Samsung Galaxy Tab), Personal Digital Assistants (PDA), peripheral devices like a Universal Serial Bus (USB) storage device and external hard drives.

Risks

3. Risks to sensitive information can be said to fall into three broad categories:

    - Confidentiality – disclosure to anyone not authorised to access the data.
    - Integrity – corruption of data by, for example, unauthorised malicious or accidental changes.
    - Availability – making data unavailable for its intended use. Examples include partially or fully deleting it, maliciously encrypting it, or preventing access by a denial-of-service attack.

    Due to these risks, users should consider the following:

    i. Sensitive information should not be stored on or accessed from mobile devices.

    ii. If sensitive information must reside on a mobile device, it should be encrypted. The decryption key should be entered manually; this step should not be automated. A means should exist to recover encrypted data when the decryption key is lost.

    iii. Sensitive information residing on mobile devices should not be the only copy. Make sure there is another copy on a more secure device such as a server that is backed up regularly.

    iv. Any sensitive information transmitted to or from the mobile device should be encrypted and/or transferred with a secure data transfer utility. Use a secure connection or protocol, such as SSL, that guarantees end-to-end encryption of all data sent or received. Devices with wireless capability pose an additional risk of unauthorised access and tampering. These capabilities should be disabled, secured, or protected with a firewall. Note that Wireless Equivalency Privacy (WEP) is inadequate protection for a wireless device transmitting sensitive information.

v. Access to the mobile device should be protected by the use of a password or in the case of a mobile phone a four digit pin.

vi. On mobile devices, do not automate the supplying of passwords or other security credentials needed to access sensitive data (for example, automatically authenticating to an application or database that contains sensitive information, or having Microsoft Windows store passwords to these systems). Likewise, any software installed on mobile devices that uses script files (a series of commands that are run when the script file is executed) should not contain a user ID or password.

vii. Reasonable care should be taken when using mobile devices in public places, meeting rooms, or other unprotected areas to avoid the unauthorised access to or disclosure of the information stored on or accessed by the device. Similar precautions should be taken when using the University's wireless network.

- Special care should be taken in crowds, meetings, and security-screening areas to maintain control over the device. Do not let it out of your sight.
- Mobile devices owned or issued by the University should not be left unattended and, where possible, should be physically locked away or secured.
- Mobile devices should be transported as carry-on luggage whenever travelling by commercial carrier unless the carrier requires otherwise.
- All mobile devices should be kept out of sight and covered when stored in a locked vehicle.
- All University-owned mobile devices should be permanently marked as University property and indicate a method of return in case the device is lost.

viii. Any mobile device capable of using antivirus software should have the software installed and configured to provide real-time protection and maintain updated virus signatures.

ix. A procedure should be established and implemented to ensure that all security patches and updates relevant to the device or installed applications are promptly applied. The patching process should be automated whenever possible. The system should be rebooted immediately after patching if required for the patch to take effect.

x. Whenever available for a mobile device, firewall software should be installed and used. Microsoft Windows, Apple Mac OS X, and Linux operating systems all have built-in firewall software that meets this guideline.

xi. Any services on the mobile device that are not needed, especially those that involve communications like 802.11 wireless, infrared, Bluetooth, remote access, FTP, or other connection functions, should be turned off.

xii. All University-owned mobile devices should be returned to the University of Kent immediately upon termination of the assigned user's relationship with the University. If the mobile device

contains sensitive information and the device will not be re-used immediately by someone authorised to access the information, the sensitive information should be removed in a manner that prevents recovery.

xiii. All University-owned mobile devices should be added to the departmental asset register.

xiv. Mobile devices and other electronic equipment that contain or access sensitive information, or have been used to access sensitive information in the past, should be processed to ensure all data is permanently removed in a manner that prevents recovery before they are disposed of.

xv. All University-owned laptop computers containing sensitive information should use tracking and recovery software, such as "Computrace" by Absolute Software Corp. (www.absolute.com), to aid in the recovery of the laptop if it is stolen or lost. Even laptops that do not contain sensitive information should consider using tracking software.

xvi. Data on mobile devices should be regularly backed up.

Connection of Personal Computer

4. All computers and mobile devices connected to the network must be electrically safe in accordance with the University Health and Safety Policy which is updated from time to time and can be found on the Safety Health and Environment Unit's website, and the manufacturers' recommendation and any applicable statutory regulations or laws.

5. All mobile device users are bound by the *Regulations for the Use of Information Technology (IT) Facilities at the University of Kent*.

6. Individuals are expected to ensure the device is in good order:

    - That they have the latest and all necessary critical security updates installed;
    - That they are using a suitable internet connection firewall (where appropriate);
    - That they are using an appropriate anti-virus with up-to-date virus definitions (where appropriate);
    - That they are using an appropriate anti-spyware/malware programme (where appropriate) and schedule scans regularly;
    - That if the device becomes infected with a virus or other malware infection, that they take appropriate action or seek advice to disinfect the device before its reconnection to the network.

7. Users must not connect a (or any) wireless broadcast device in infrastructure mode (ie WiFi access points) on campus.

8. Users must not adversely interfere with the use of the network by others or interfere in any way with the running of the network, or contravene any other regulations including JANET Acceptable User Policy and other University of Kent or any statutory regulations or laws.

Withdrawal of Access

9. Information Services takes misuse/abuse very seriously - actions that disrupt network facilities may lead to withdrawal of access or the temporary or permanent withdrawal of any or all of the following:

    - VPN access
    - Access to the Study Bedroom Network
    - Wireless access
    - Your Kent IT Account.

Approved 23 March 2012