Information Services

Regulations for the Use of Computers & Mobile Devices Not Owned and/or managed 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 personal computer and/or mobile devices to connect to the University of Kent Network

    - All users of virtual private networking (VPN), dial-up or other technologies used to access University IT systems using a personal computer and/or mobile device.

    - All users connected to the Study Bedroom Service.

    - All users connected to the wireless network

    - All users directly connecting a personal computer and/or mobile device to the University network.

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 Samson Galaxy Tab), Personal Digital Assistants (PDA), peripheral devices like Universal Serial Bus (USB) flash drives.

Liability

3. Connecting your personal computer and/or mobile device to the University of Kent network is entirely at the risk of the user. The University will not be liable for any loss, damage or inconvenience arising directly or indirectly to a personal computer and/or mobile device as a result of its connection to the network. Although the University takes reasonable care to prevent the corruption of information, the University does not give any warranty or understanding to the user about the integrity of information.

4. The University accepts no responsibility for the malfunctioning of a personal computer and/or mobile device, its hardware or software as a result of its connection to the University of Kent network.

5. The University accepts no responsibility for the loss of any data or the failure of any security or privacy mechanism on a personal computer and/or mobile device that has been connected or is connected to the University of Kent network.

Connection of Personal Computer

6. 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.

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

8. Individuals are expected to ensure the personal computer and/or mobile 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 they become infected with a virus or other malware infection, that they take appropriate action to disinfect their machine/device before its reconnection to the network.

9. Users may only connect one computer or mobile device to a network point.

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

11. 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.

Risks associated with using a mobile device

12. Risks to sensitive/confidential 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 adhere to the following:

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

ii. If sensitive/confidential 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/confidential 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/confidential 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 using a password in the case of a computer and a four digit pin (personal identification number) in the case of mobile phones. At minimum only secure flash drives should be used that allow a five-key pin or the more sophisticated version that uses a 10-key pin (ensuring data remains encrypted until the correct pin is entered)

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/confidential 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.

- 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.

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 wireless, infrared, Bluetooth, remote access, FTP, or other connection functions, should be turned off.

xii. Mobile devices and other electronic equipment that contain or access sensitive/confidential information, or have been used to access sensitive/confidential 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.

xiii. The University strongly recommends that users with mobile devices should consider using tracking and recovery software to aid recovery if it is stolen or lost. Even laptop computers that do not contain sensitive information should consider using tracking software.

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

Withdrawal of Access

13. 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