Guide to Information Security for Mobile Devices

Background

There have been a number of stories in the press and media in recent years about personal and confidential data being lost whilst in transit, laptops left in cafes, child benefit data CDs being lost. Such losses cause public anxiety around identity theft, undermine the confidence and reputation of organisations involved and can potentially lead to litigation and severe penalties.

The problems of moving data about securely are not new but the technologies available are changing. For example, new mobile devices such as Smart phones have capabilities for information access and mass storage and present risks similar to laptop computers. The purpose of this leaflet is to give some guidance to staff and research students on recommended practice around using mobile devices to store documents, files or data.

The guidance should be read in conjunction with the University's Information Security Policy and Data Protection Policy.

What are Mobile Devices?

For the purpose of this guidance, mobile devices are classified as any device holding data which is likely to be carried from place to place and includes:

- Laptop computers, tablets, handheld computers (especially PDAs)
- USB Pen drives
- Mobile phones (especially smart phones)
- CD/DVD ROMs
- portable hard drives

These portable devices are more prone to being lost due to the nature of their portability. Laptops, phones and hard drives are highly desirable and therefore attractive to thieves.

You must assume that in the case of loss or theft, the data stored on these devices is potentially then accessible to unauthorised people. For this reason it is essential that you are aware of the risks and take extra precautions.

Responsibility

Anyone who stores, or transports data and information concerned with the operation of the University, using mobile devices is deemed by the University to be responsible for the security of that data in transit and must take adequate and appropriate steps to safeguard it. If there is a loss or unauthorised disclosure of confidential, sensitive or personal data from the University due to poor practice or negligence on your part, disciplinary action may be taken against you, where the ultimate sanction is dismissal from the University.

Required Practice

All users are required to abide by the following practices.

1. You must not store confidential/sensitive or personal data e.g. info relating to living individuals that has been provided the University, on a mobile device without prior authorisation from the data owner or custodian. You may not save copies or extracts of student or staff records, exam marks etc without expressed permission.

    a. confidential/sensitive or personal data stored on a mobile device, must be encrypted using a minimum of AES 128 bit encryption with a strong key/password of at least 10 characters (see password guidelines).

    b. Microsoft office 2007 provides a facility to encrypt word and excel files in AES 128 and provides an easy secure option for documents

    c. AES 256 bit USB pen drives are available widely and are recommended. Some models will destroy the data after six failed attempts to crack the password. Other secure USB drives with combination locks etc have been show to be easy to hack and should be avoided.

2. Any device that pulls e-mail from the University systems e.g. Smartphone, Blackberry, iPhone etc, whether owned by the University or by the individual, must be effectively protected with a system authenticated password.

3. Sensitive or confidential data should, ideally, not be passed by e-mail. Where this unavoidable, it must be encrypted.

4. Disable Wi-fi and Bluetooth when you don’t need them. Not only does this make your mobile device more secure but saves on the battery use. Disabling/enabling these features varies from device to device - your lap-top and Smartphone manuals will contain the details.

5. Avoid accessing or transmitting sensitive/confidential data when connected to public and open wi-fi hot spots.

6. When using your laptop in public spaces e.g. on trains, airport lounges, you must take care over what can be seen on your screen.

7. Care should be taken to protect mobile devices from theft:

    - Lock laptops, and tablet computers in the boot when parked or travelling by car
    - Don't leave your phone in an unattended car - 50% of all mobile thefts are from vehicles
    - Take extra care and be vigilant in public spaces and on public transport
    - Make sure you lock the office door when leaving equipment unattended

8. All lost or stolen devices that contain confidential, sensitive or personal data belonging to the University must be reported immediately to the Head of Information Systems, Technology and Library and where appropriate (laptop, phone) to the police.

9. Mobile phone apps represent a new risk from malware and viruses. Downloaded apps can incorporate undesirable code which open your phone up for hacking. Only buy from dedicated app stores and avoid downloading pirated apps. Be cautious and wary of software downloads and their origins.

10. E-mail concerning University business is discoverable under freedom of information and data protection legislation. Therefore you must take care when writing e-mails, not to liable or be derogatory about individuals or organisations. Always assume that those mentioned in an e-mail are free to read the e-mail if they so wish.

Classification of data for security purposes

1.	Confidential/Highly sensitive	Data which may or may not be personal and which should not be disclosed except where authorised e.g. application data, examination papers, student mark profiles prepared for examination boards, disciplinary proceedings or investigations
2.	Sensitive	Personal data consisting of information relating to religious belief, political opinions, sexuality, physical or mental health, court action etc
3.	Personal	Data which enables individuals to be identified or relates to an identifiable individual. This can be processed lawfully by the University provided that staff comply with the DPA and the University's notification.
4.	Internal	Data which is concerned with the running of the University prior to it becoming public domain e.g. committee papers
5.	Unclassified /Public domain	Information which is not confidential or personal and which may be disseminated within the University and without.

Explanation of Encryption

Encryption is a process that converts a document, message or other computer files into an unreadable cipher that can only be decoded using a key code (often a password). The key code has to be shared with the person who needs access. AES-128 is recognised secure standard for encryption that is widely supported in office applications or for encrypting devices e.g. you can buy AES-128 pen drives. Encrypted documents could still be hacked using a computer programs that tries different passwords (a brute force attack), but the longer and more complicated the password, the longer it will take a computer to try different combinations. A brute force attack, on a complex and strong password of 10 characters (letters, numbers and symbols) will take many taking years of computing power to break. It is also critical to keep the key code confidential and restricted to only those that need to know.

This Policy to be Read by:	
Staff	✓
Students	✓
Governors	✓
Consultants	✓
Partner staff of the University of Bolton	✓
Contractors of the University	✓

Document History

Document last edited by po1 at 19/03/2012 12:58:00