The University of Manchester

MANCHESTER 1824

IT SECURITY
Guide to data handling

You are responsible and liable for the data you handle, not your line manager or the University

1. Physical Security

Your PC or laptop should be secured and your office locked at night. If you take your laptop home or away on business keep it secure at all times. Other devices such as PDAs, USB drives and CDs should be kept secure at all times.

2. Sensitive Data

If you have sensitive data on a laptop or other mobile device such as a USB drive, CD or PDA ask: Why? Do you currently need it for your job? If not, remove or destroy it.

Q: What is sensitive data?

A: There are lots of classification systems but use common sense - for instance does the data include personal information? Simply decide if data is either sensitive or non sensitive. Your line manager or the Records Management Office should be able to provide guidance on what is sensitive data.

If in doubt, treat as sensitive.

3. Laptops

If your laptop holds sensitive data needed for your job it needs to be encrypted using University prescribed software or software which is compliant with or recommended by an approved 3rd party such as an NHS Trust.

4. PDAs, Mobile Phones

Do not keep sensitive data on PDAs or mobile phones.

5. USB Device including USB pens and drives

If your USB device holds sensitive data needed for your job it needs to be encrypted using University approved software.

6. CDs, DVDs and other media

If you need to create sensitive data files on a CD, DVD or other media ensure the data file is encrypted using either University approved software or software which is compliant with or recommended by an approved 3rd party such as an NHS Trust.

7. Email Attachments

If you need to send sensitive data by email ask: Is it really necessary? Can it be depersonalised or aggregated? If in doubt treat as sensitive and ensure the data file is encrypted using either University approved software or software which is compliant with or recommended by an approved 3rd party such as an NHS Trust.

If you are not following these guidelines you should not be sending sensitive data by email. Sensitive data should be sent as an encrypted attachment and not in the body of the email itself.

Q: What is encryption?

A: Converting data into a coded form that can not be read without knowing a password or phrase (key).

Link to related documents and advice
www.manchester.ac.uk/secure-it

This includes this guide, guidance to software identified in this guide, links to the IT Security Policies and how to get further assistance if required.

SECURE IT