The University of Manchester

MANCHESTER 1824

IT SECURITY

Guide to protecting data using encryption

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

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

Why do I need to use encryption?

Sensitive data should be protected so that unauthorised persons cannot access it. Sensitive data held on devices such as laptops, USB sticks, mobile phones or PDAs, is at risk if the device is lost or stolen.

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.

What can I encrypt?

The disks on PCs, laptops and USB sticks can be fully encrypted so that any data stored on the device is automatically encrypted. A password or phrase (key) is needed to unlock the contents of the device.

Individual files and documents can also be encrypted. A password or phrase (key) is required to decrypt the document. The user must remember to encrypt the document and ensure that only the encrypted version is kept on any portable devices.

What password should I use?

Protection provided by encryption is only as strong as the password or pass phrase used. The longer and more complex (mix of letters, digits, punctuation etc) the stronger the protection. Passwords should not be easily guessable.

What if I forget my password or phrase (key)?

Modern encryption techniques are virtually unbreakable and so if you lose your password to an encrypted device or document, the contents are lost forever! ***IT staff cannot help in recovering encrypted data.***

Do not encryt the only source of the data, you should make sure you keep an unencrypt copy of the data on a secure server at the University (eg P-drive).

What if I need to share encrypted data?

If you need to share encrypted documents with others, then you will need to tell them the password or phrase (key). Sharing by telephone or text after verifying you are communicating with the right person is ideal. Never send passwords by email.

Remember the password you use to logon to University systems should never be shared with anyone!

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

SECURE IT