MANCHESTER
1824

The University of Manchester

IT SECURITY

Guide to email and sensitive data

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

Email is not a secure way of transmitting data, so we recommend you don't use email to send sensitive data unless you have to. A secure way to share data is to use shared folders (on secure University servers or LiveLink) and to only email the location of the relevant data.

Who, what, why and how

If you are about to send sensitive data to someone via email then pause and ask:

Who? Who am I sending this to? Am I sending it to the correct address?
Is the recipient entitled to see this data?

What? What data am I sending? Is it considered sensitive? Could it be anonymised before sending?

Why? Is there a strong business case for sending this data by email?
Could it be made available some other way (e.g., via a secure WEB site)?

How? How do I ensure the data is secure?

If after answering these questions you still need to send the data by email then you should follow this advice.

1. Who?

Check the recipient's email address before hitting the send button. Make sure you do not send sensitive data to the wrong person or persons.

Unless there is a strong business need, sensitive data should not be sent to people outside the University.

2. What?

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.***

Ensure you send the data as an encrypted attachment (never as the body of the email) using either University prescribed software or software which is compliant with or prescribed by an approved 3rd party such as an NHS Trust.

3. Why?

Finally, make sure there is a real need to send this data, and if so carry out the checks prescribed here and employ suitable tools to protect the data.

4. How?

University prescribed encryption software to encrypt one or more files before sending.

Use strong complex passwords which cannot be easilly guessed. Passwords should be communicated (telephone, text) to the recipient and never be sent by email.

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

If you are not following these guidelines you should *not* be sending sensitive data by email.

Link to related guidance including how to obtain and use the prescribed encryption software.
www.manchester.ac.uk/secure-it

SECURE IT