# Information Security

Information Security at the University is extremely important – the loss or unauthorised disclosure of information poses significant reputational and financial risks. The use of portable devices (e.g. Laptops and USB sticks) increases these risks further. Misuse of information runs the risk of undermining public trust in the University, and its ability to attract funding.

The Information Commissioner's Office can implement fines of up to £500,000 for serious breaches of the Data Protection Act which could have been preventable. This includes accidental faxing/emailing of personal information to incorrect recipients and the theft from an employee's home of an unencrypted laptop with sensitive personal data.

In order to comply with University policy and to keep confidential data safe, please read and abide by the following...

## Hard Copies

- If copying confidential information, only ever make as many copies as you need, keep a record of those copies.
- Delete/destroy copies once they are no longer needed
- Shred confidential documents
- Mark any hard copied containing confidential information as 'CONFIDENTIAL'
- Store confidential information in locked cupboards/cabinets, or if this is not possible then a room which is kept locked when unoccupied
- Don't leave hard copies of confidential documents unattended
- Ensure the recipient is clearly stated when sending documents using internal/external mail. Include 'confidential' on the sealed envelope if necessary

## IT Procedures

- Use strong passwords that aren't easily guessable and don't share them with anyone
- Don't leave you computer logged on and unattended
- Use antiviral software and keep it updated!
- Keep firewalls turned on
- Regularly install updates
- Don't follow links or open attachments on unsolicited emails
- Don't install pirate software
- Only visit reputable websites
- Only use USB devices that you know are safe in your machine
- Keep backups
- Ensure personal computers are virus free and protected if working remotely
- Use dedicated storage e.g. file servers as opposed to local hard disks
- Mobile devices containing personal information must be encypted
- **If you have any suspicions have IT staff investigate them**

Be mindful of where you are when discussing confidential information

PLEASE FAMILIARISE YOURSELF WITH THE UNIVERSITY INFORMATION SECURITY POLICY AT http://www.it.ox.ac.uk/infosec/ispolicy/ AND ENSURE YOU FOLLOW IT AT ALL TIMES!