

## Encrypting documents in Office 2007

### Why Encrypt?


To comply with the Data Protection Act and University Regulations, data classified as *confidential or above* **should be encrypted** when transported or saved in a non-secure location. For example, when sent by email, saved onto a memory stick, or saved onto a laptop, netbook or other portable device. For further information see: <http://www.bristol.ac.uk/infosec/uobdata/encrypt/>

### What is encryption?

**Encryption** is the process of converting data into a format that is unreadable by others. The information only becomes useable again when it is **decrypted** by an authorized user who has the password. Word, Excel and PowerPoint 2007 offer encryption facilities which meet University encryption standards.

### Encrypting a document using Word, Excel or PowerPoint 2007

The file must be in the **new** file format, eg .docx for a Word document. Files saved in Compatibility Mode, or the 97-2003 file format do not have adequate encryption facilities.

1. With the relevant document open, click on the **Office Button** 
2. Click on **Prepare**, then click on **Encrypt Document**, as shown in Figure 1
3. Enter a 'strong' password (see [Choosing a password](#))
4. Click **OK**, re-enter the password, then click **OK** again.
5. The document is now encrypted and the password will be required to open it.

Note that you do not need the password to delete the file or to save changes to it, just to open it.

**WARNING! AFTER A DOCUMENT IS ENCRYPTED, WITHOUT THE PASSWORD, THE DATA IS LOST AND TOTALLY IRRETRIEVABLE.**

Note that protecting a document from modification by others is not the same as encrypting it.

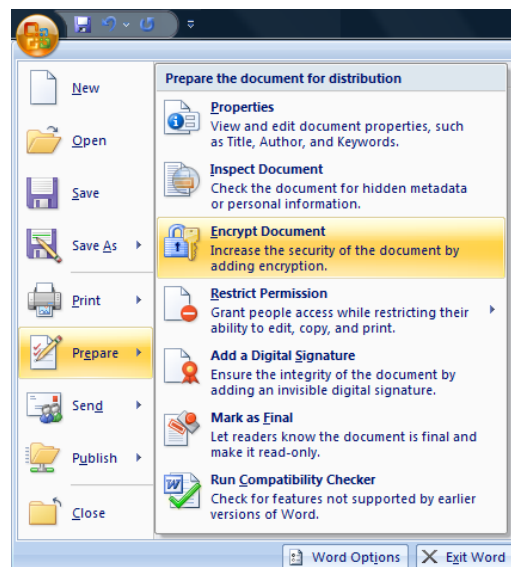


Figure 1 - Encrypt Document option in Word 2007

### Choosing a password

Any passwords you use should be 'strong'. This means they should be impossible to guess. For advice on choosing a password, see: <http://www.bristol.ac.uk/infosec/protectyou/passwords/>

### Sharing passwords

If the document needs to be shared with others, then obviously so does the password. Share it using a mechanism different to the way you are sharing the file. For example, if you email an encrypted document, phone someone to give them the password.

If the only copies of your documents are encrypted then you need to consider the security of the encryption passwords themselves and it is recommended that you lodge these securely with a trusted third party (who, preferably don't have access to the documents) so as to ensure their availability in the event of password loss.

### University's Security Awareness Website

Everyone should familiarise themselves with the contents of University's Information Security website: <http://www.bristol.ac.uk/infosec/>