Remember, data security is your responsibility!

Everyone should familiarise themselves with the contents of the University's Information Security website section:

www.bristol.ac.uk/infosec/

Top Ten Tips

- ✓ **Know what constitutes restricted data**
- ✓ **Process restricted data on secure UOB computers only and do not store restricted data on non-UOB equipment**
- ✓ **Encrypt restricted data to transport or convey it and fully disk encrypt your laptop/ netbook**
- ✓ **Share restricted data only with those with the right and need to view it**
- ✓ **Do not make copies of restricted data**
- ✓ **Lock away unsecured restricted data and lock your door if leaving your room unattended**
- ✓ **Never share or disclose your UOB password or use it for non-UOB services**
- ✓ **For UOB business use your UOB email account and a UOB-recommended secure email client**
- ✓ **Securely erase data before disposing of hardware and storage**
- ✓ **If in doubt about data, ask advice from your departmental data protection advisor**

University of
BRISTOL

IT SERVICES

Encrypting documents in Office 2013 & 2010

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 authorised user who has the password. Word, Excel and PowerPoint 2013 & 2010 offer encryption facilities which meet University encryption standards.

Why Encrypt?

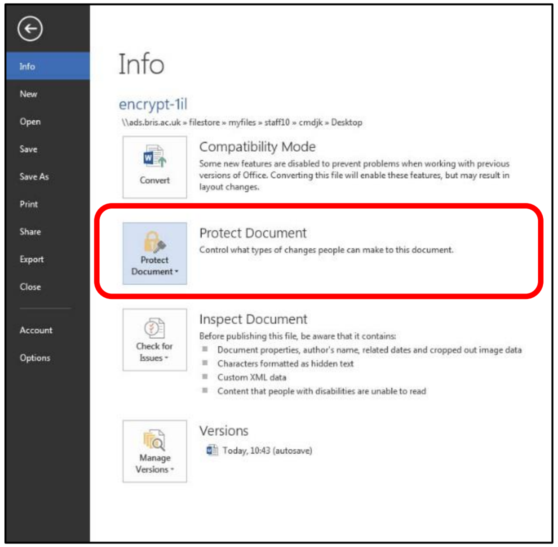
To comply with the Data Protection Act and University Regulations, data classified as **confidential, or above, should be encrypted** when transported or saved in a non-secure location. For example, when sent by email, saved onto a memory stick, or saved onto a laptop, netbook or other portable device.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

March 2015

Encrypting a document using Word, Excel or PowerPoint 2013

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 **File** menu
2. If not already selected choose **Info**, then click on **Protect Document**, as shown in *Figure 1*



Some new features are disabled to prevent problems when working with previous versions of Office. Converting this file will enable these features, but may result in layout changes.

Control what types of changes people can make to this document.

Before publishing this file, be aware that it contains:

- Document properties, author's name, related dates and cropped out image data
- Characters formatted as hidden text
- Custom XML data
- Content that people with disabilities are unable to read

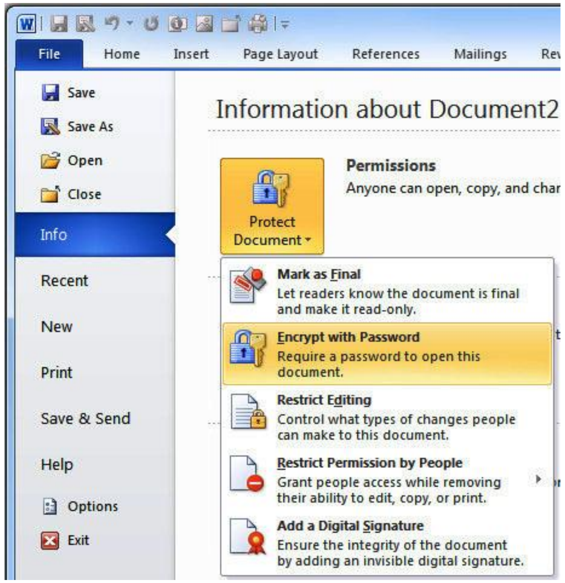
Figure 1 - Protect Document option in Word 2013

3. Enter a ‘strong’ password (see the section **Choosing a password**)
4. Click **OK**, re-enter the password, then click **OK** again.
5. Save the document.
6. The document is now encrypted and the password will be required to open it.

Encrypting a document using Word, Excel or PowerPoint 2010

The file must be in the **new** file format, eg .docx for a Word document.

1. With the relevant document open, click on the **File Tab**
2. Click on **Info**, click on **Protect Document** and then **Encrypt with Password**, as shown in Figure 2



Anyone can open, copy, and char

Let readers know the document is final and make it read-only.

Require a password to open this document.

Control what types of changes people can make to this document.

Grant people access while removing their ability to edit, copy, or print.

Ensure the integrity of the document by adding an invisible digital signature.

Figure 2 - Encrypt Document option in Word 2010

3. Enter a ‘strong’ password (see the section **Choosing a password**)
4. Click **OK**, re-enter the password, then click **OK** again.
5. Save the document.
6. The document is now encrypted and the password will be required to open it.

WARNING!

AFTER A DOCUMENT IS ENCRYPTED: WITHOUT THE PASSWORD THE DATA IS LOST AND TOTALLY IRRETRIEVABLE

Please note:

1. You do not need the password to delete the file or to save changes to it, just to open it.

2. Protecting a document from modification by others is not the same as encrypting it.

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: www.bristol.ac.uk/infosec/protectyou/passwords

Sharing passwords

If the document needs to be shared with others, then obviously so does the password (only share it with those authorised to access the data). Share the password using a mechanism which is 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 and authorised third party (who, preferably, doesn't have access to the documents) so as to ensure their availability in the event of password loss.