DATA ENCRYPTION GUIDE

Table of Contents

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 the College's encryption standards
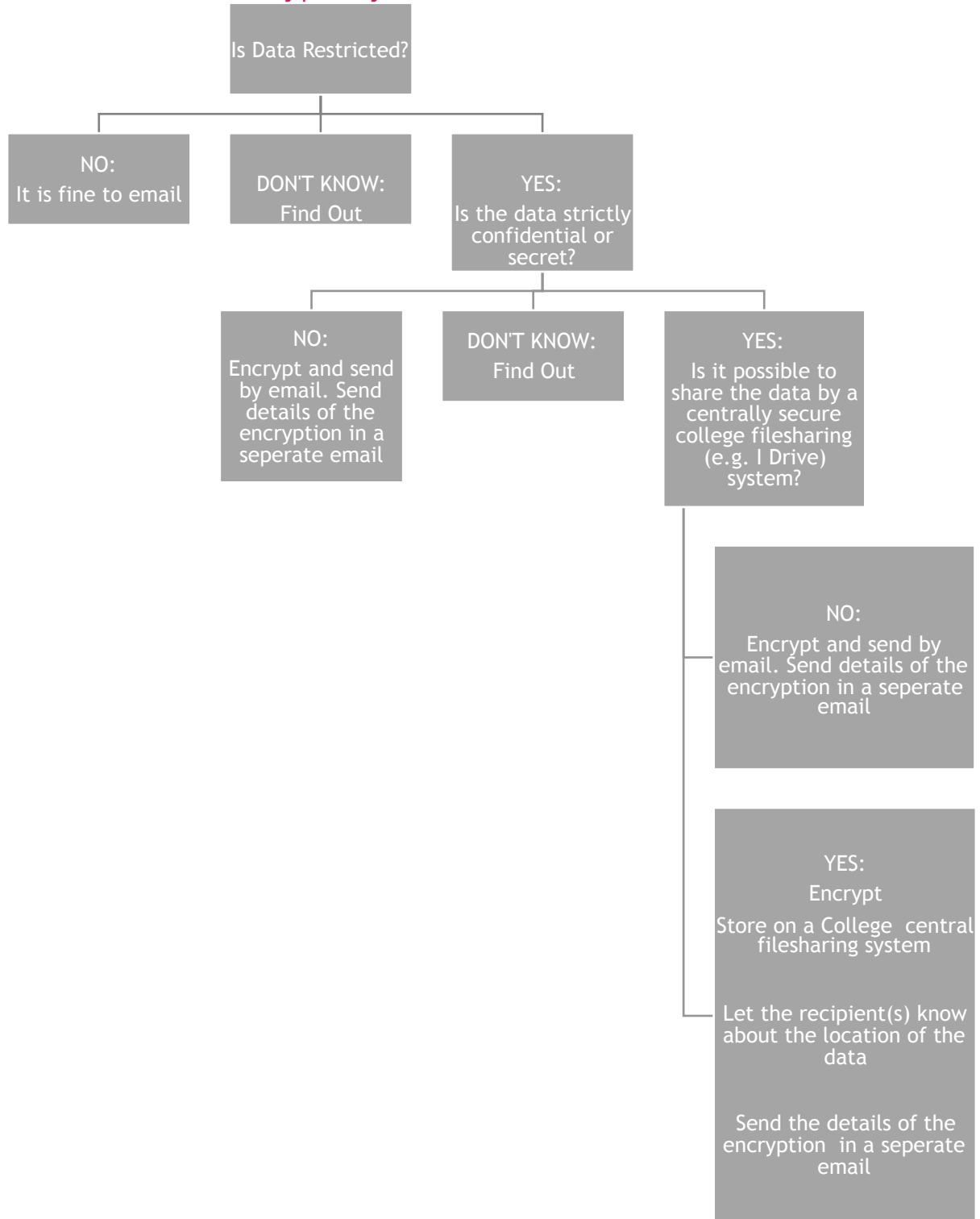
Why Encrypt?

To comply with the Data Protection Act and College 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.

Encryption is a means of preventing anyone other than those who have a key from accessing data, be it in an email, on a computer or on a storage device. In all cases you need to consider the security of the encryption key(s) and it is recommend that you lodge these securely with a trusted third party (who, preferably doesn't have access to the files) so as to ensure their availability in the event of key loss.

Top Ten Tips for Data Encryption

- Know what constitutes restricted data
- Process restricted data on secure College computers only and do not store restricted data on non-College 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 College network password or use it for non-College services
- For College business use your College email account and a College-recommended secure email client (i.e. Outlook)
- Securely erase data before disposing of hardware and storage
- If in doubt about data, ask advice from IT Services

Do I Need to Encrypt my Data?

Is Data Restricted?

NO:
It is fine to email

DON'T KNOW:
Find Out

YES:
Is the data strictly confidential or secret?

NO:
Encrypt and send by email. Send details of the encryption in a seperate email

DON'T KNOW:
Find Out

YES:
Is it possible to share the data by a centrally secure college filesharing (e.g. I Drive) system?

NO:
Encrypt and send by email. Send details of the encryption in a seperate email

YES:
Encrypt

Store on a College central filesharing system

Let the recipient(s) know about the location of the data

Send the details of the encryption in a seperate email

Encrypting a document using Word, Excel or PowerPoint 2013

Step 1: 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.

Step 2: With the relevant document open, click on the *File* menu

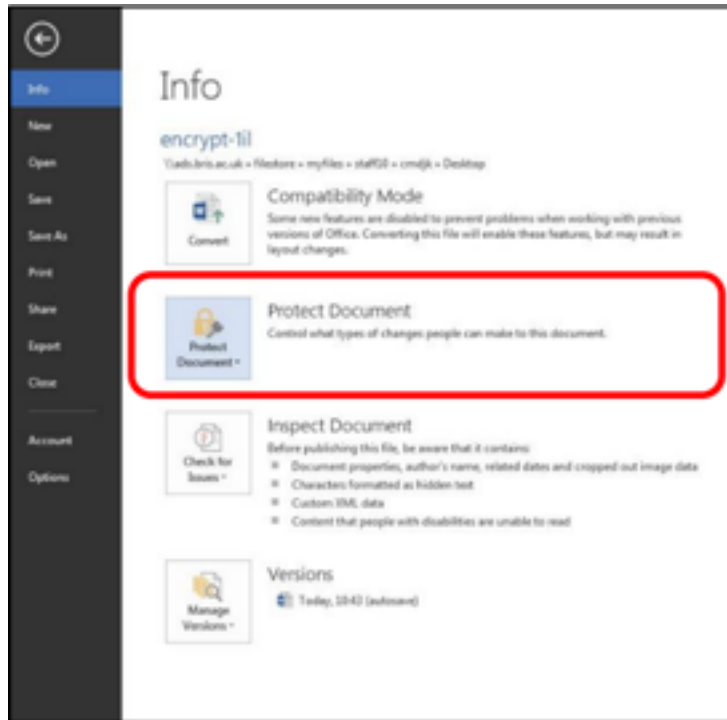Step 3: If not already selected choose Info, then click on Protect Document, as shown in Figure 1

Figure 1. Protect Document Option in Office 2013

Step 4: Enter a 'strong' password (see the section Choosing a password)

Step 5: Click **OK**, re-enter the password, then click **OK** again.

Step 6: Save the document.

Step 7: The document is now encrypted and the password will be required to open it.

Encrypting a document using Word, Excel or PowerPoint 2010

Step 1: 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.

Step 2: With the relevant document open, click on the *File* menu

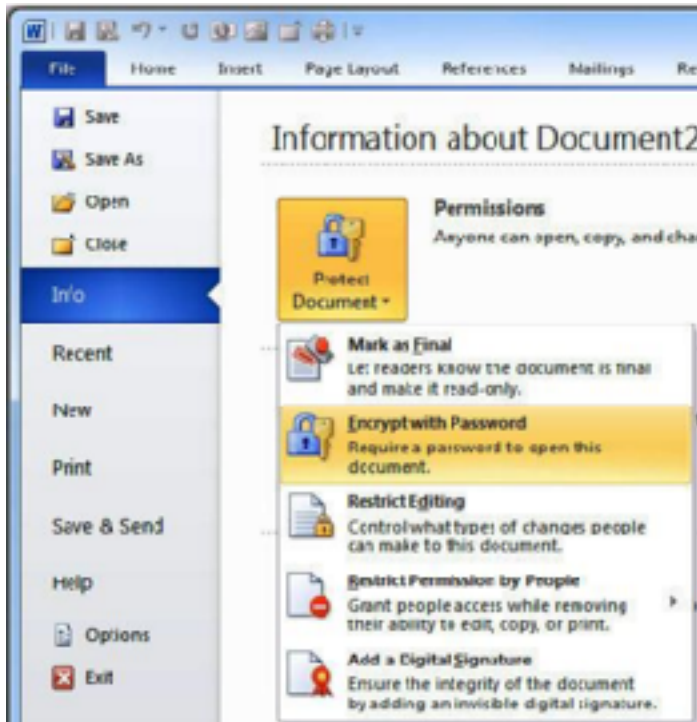Step 3: If not already selected choose Info, then click on Protect Document, as shown in Figure 2

Figure 2. Protect Document Option in Office 2010

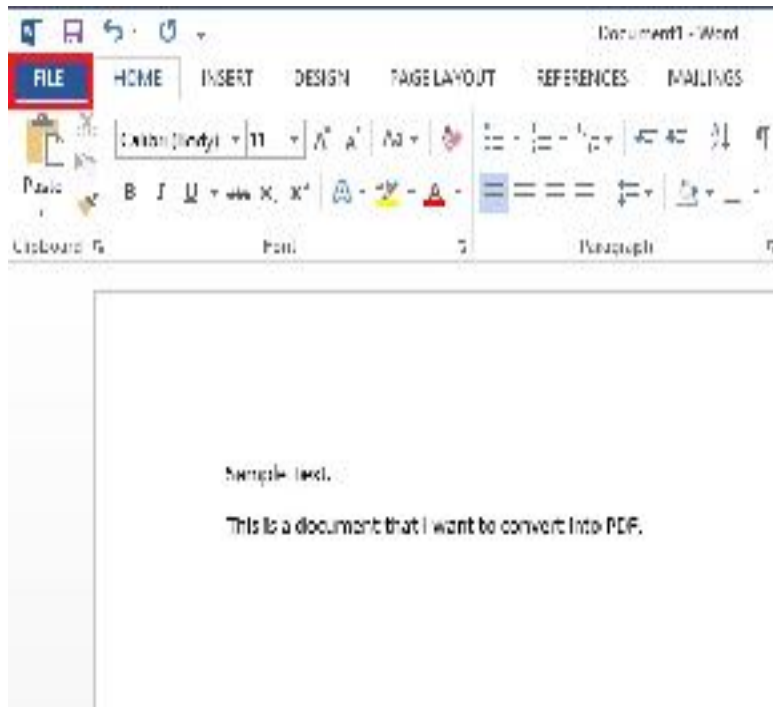Step 4: Enter a 'strong' password (see the section Choosing a password)

Step 5: Click **OK**, re-enter the password, then click **OK** again.
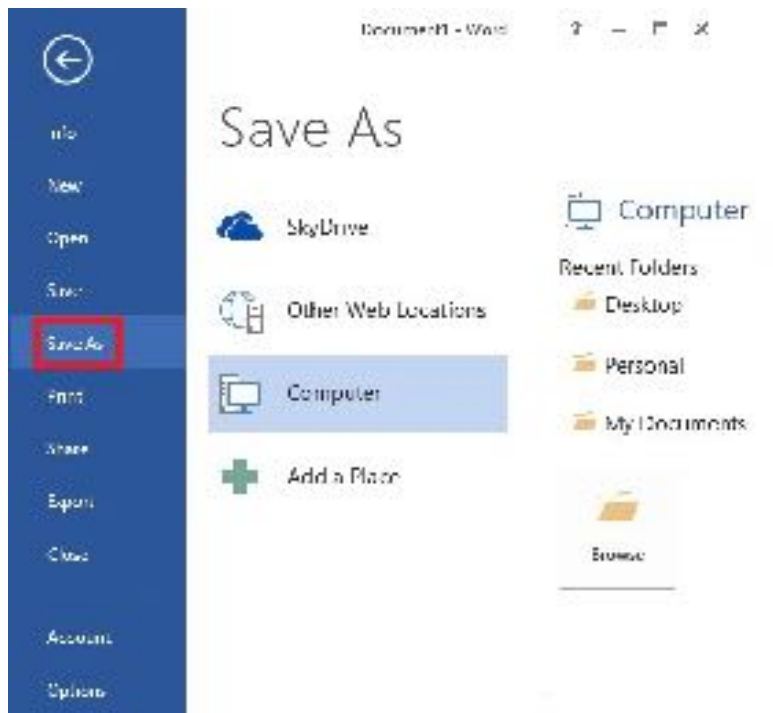
Step 6: Save the document.

Step 7: The document is now encrypted and the password will be required to open it.

Encrypting a PDF document using Microsoft Word

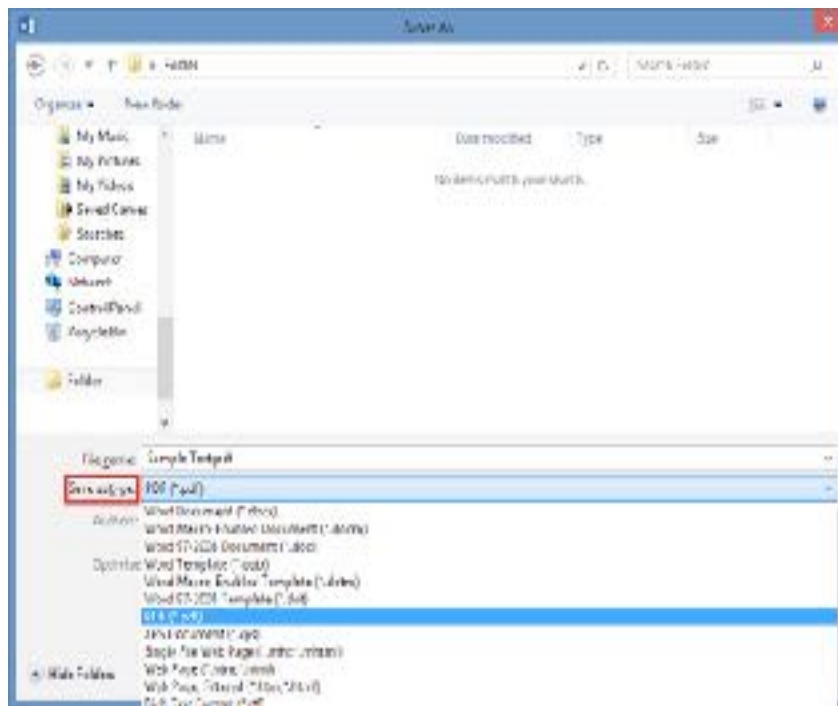**Step 1:** Open you Microsoft Word Document as shown below

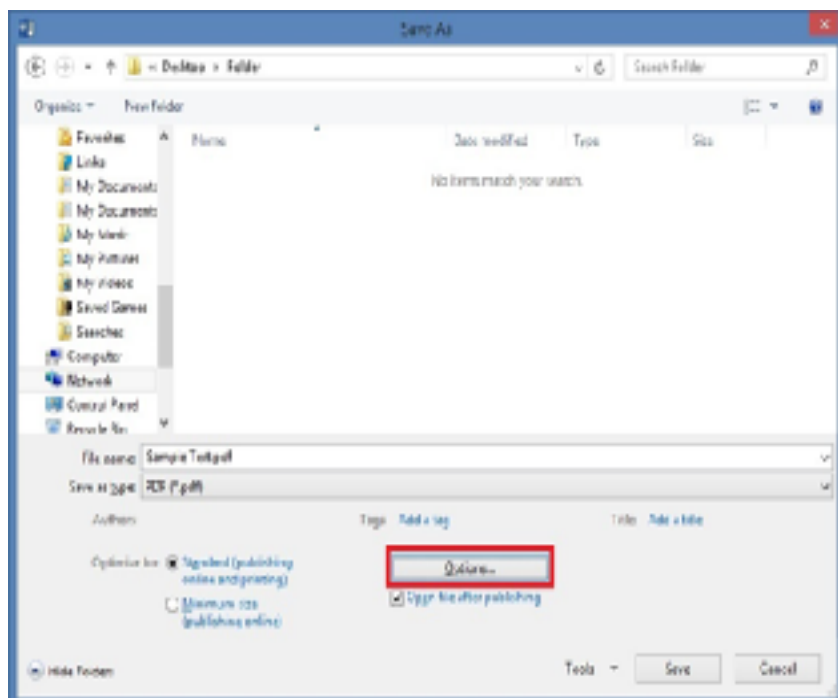**Step 2:** Click **Save As** and then choose a desired location for the document to reside

Step 3: From the "Save As" dialogue box, select PDF from the "Save as type" dropdown list.
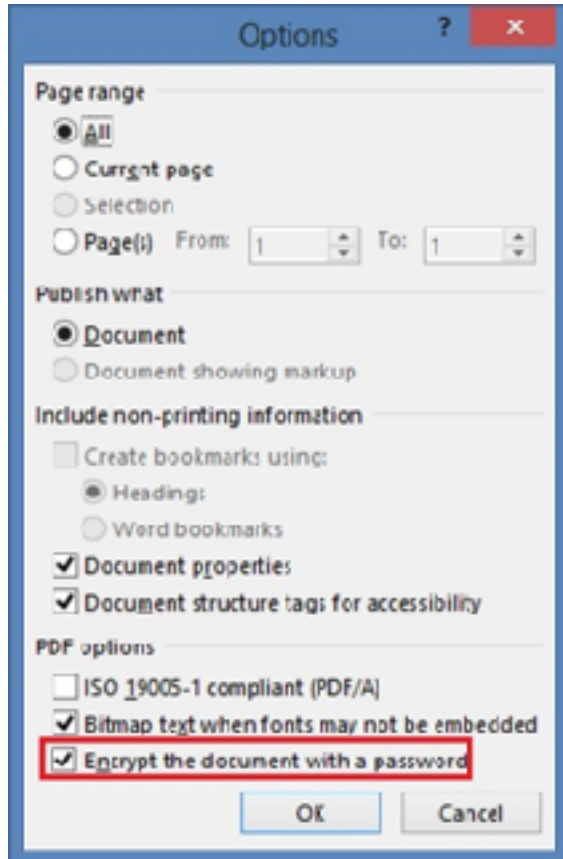

Step 4: Click the **Options**... button.

Step 5: From the "Options" dialogue box, check Encrypt the document with a password.

Step 6: You are now prompted to enter a password. Once finished, click **OK**.

Step 7: The document is now encrypted and the password will be required to open it.

> **WARNING!**
> **AFTER A DOCUMENT IS ENCRYPTED: WITHOUT THEPASSWORD 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

Using a weak password that can be easily guessed is not a sensible move. Remember, there are many applications that can generate and test millions of passwords per hour. Even strong passwords are not infallible, but they make things as difficult as possible for a hacker. Further information about choosing a strong password can be found in the College Information Security Guide.

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). Ideally, 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.