

### How to protect documents with passwords

Documents containing personal data should be password protected so that only the intended parties can view the information. Personal data relates to things such as names, dates of birth, addresses, telephone numbers, email addresses and so on: anything that can lead to a person being identified. It is essential that you password protect documents containing this information so as not to breach data protection laws such as GDPR ([General Data Protection Regulation](#)). It is recommended that you communicate the password separately, such as in another email, as an added layer of protection.

#### Using Microsoft office

- Open document in Word or Excel, add your information and save it to your computer or your documents.
- Re-open the document, click **File** then **Info** then choose **Permissions**.
- Click the **Permissions** option then **Protect Document**
- Choose **Encrypt with Password**
- In the pop up box type your password and click **Ok**, it will then ask you for the password a second time. Re-type it and click **Ok** again.
- The document is then password protected.

### How to remove the password or change it

- If you then want to remove the password, open the document and type in the appropriate password
- Click **File** then choose **Info** then **Permissions**.
- Click the **Permissions** option then **Protect Document**
- Choose **Encrypt with Password**
- When the pop up screen appears delete the black dots, and save the document again. The password is then removed.

- Or, to change it, type a different password and click **Ok**, it will then ask you for the password a second time. Re-type it and click **Ok** again.

It can vary very slightly with different computers or different versions of Microsoft office. For more information, see the Microsoft help section

here: <https://support.office.com/en-us/article/add-or-remove-protection-in-your-document-workbook-or-presentation-05084cc3-300d-4c1a-8416-38d3e37d6826>

### Using Apple software

- Open the document that you want to help protect.
- On the Word menu, click **Preferences**
- Under **Personal Settings**, click **Security**
- In the **Password to open** box, type a password, and then click **OK**
- In the **Confirm Password** dialog box, type the password again, and then click **OK**
- Save the document.

Further information including images of the process can be found on the Microsoft website here: <https://support.office.com/en-us/article/password-protect-a-document-in-word-for-mac-5dc20870-62ea-43b1-ab0b-39426a57cffi>

### Using BCC when you email and why you should use it.

When you are sending an email there are different fields to enter the recipients email address in. There are usually three different options:

- To
- Cc
- Bcc

Cc stands for *carbon copy* – having someone's email address in this field sends them a copy of the email. Bcc stands for *blind carbon copy* – the Bcc field is used to send a copy of the email to all the recipients **without making email addresses visible to the other recipients.**

Sometimes only the 'To' and 'Cc' fields can be seen at the top of the email you are composing. To make the Bcc field available look for the button on your toolbar at the top that says 'show fields' or 'show Bcc field'. This will be different on each email provider, but usually can be found under 'view' or 'options' tabs on the toolbar. If you are struggling to locate it, your email provider will have a help feature where you can search for your query.

When you are sending an email to just one recipient, it is fine to put their email address in the 'To' field. However, if you are sending the email to multiple recipients then the way to keep their email addresses private from each other is by entering their email addresses in to the 'Bcc' field.

For example, if you are sending out the minutes of a meeting, then the email addresses of each person receiving the minutes should be entered into the Bcc field so that when they receive the email they can only see that it has been sent to them and they cannot see email addresses of the other people receiving the email.

This is imperative to avoid sharing personal information which can be a breach of data protection. Personal information includes email addresses.