Records Management Office Documentation

Version	Date of Change	Notes	Editor
2.0	18/12/2013		Phil Oakman
2.1	07/12/2018	Updated Template	Gareth Reeves
3.0	11/02/2019	Added Appendix Three, updated to office 2016 instructions.	Gareth Reeves

Add security to confidential information to be sent via email

Contents

Introduction

In an ideal world sensitive information should not be sent by email because it isn't a secure form of communication. However, living in the real world and needing to use email there are a couple of things we can do to help maintain the security of information.

The more sensitive something is, the more control ought to be added. It doesn't matter if it is the personal data of one person or one hundred people, all personal data (especially Special Category "sensitive personal" data) should be protected and handled in a secure professional manner by University staff.

Firstly, as a way of adding to the security of the process all staff who deal with sensitive or confidential information on a regular basis should turn off the auto-complete function in Outlook so that the whole address must be typed. Carrying out this process acts as an additional check that the address is the correct one and not a similar one suggested by the auto-complete function. (See Appendix one for this process)

Secondly, staff sending out highly personal or confidential information via email should first create the text in Word and then password protect the document before attaching it to any email. (See Appendix two for this process) Where multiple documents need to be sent by email or the content is not in Word format, multiple files can be encrypted with a password ready from emailing. (See Appendix three for this process)

As an example - a member of staff in a team has an ongoing commitment to the care and supervision of a student with a health problem and will need to communicate with them on a regular basis. In this case, at the start of the business relationship the student should be issued with their own individual password which they will need to access email attachments. When any emails are sent the information should be protected within the email in a word attachment that only they can password access.
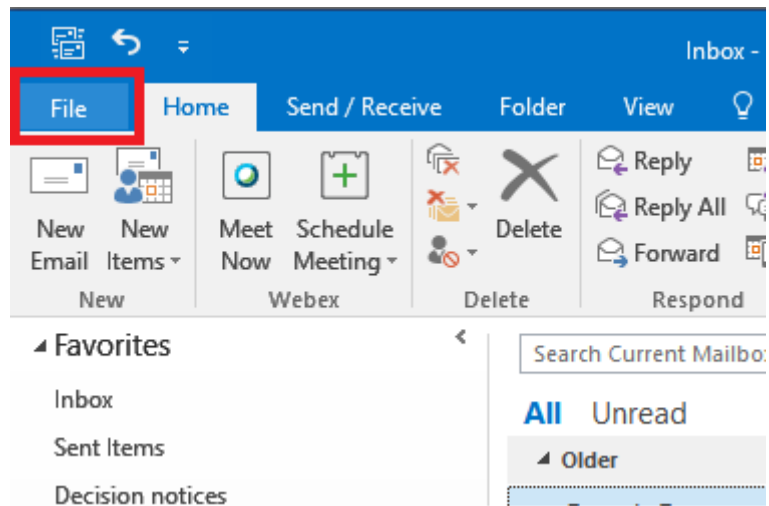
Passwords should not be sent within the same email as email attachments

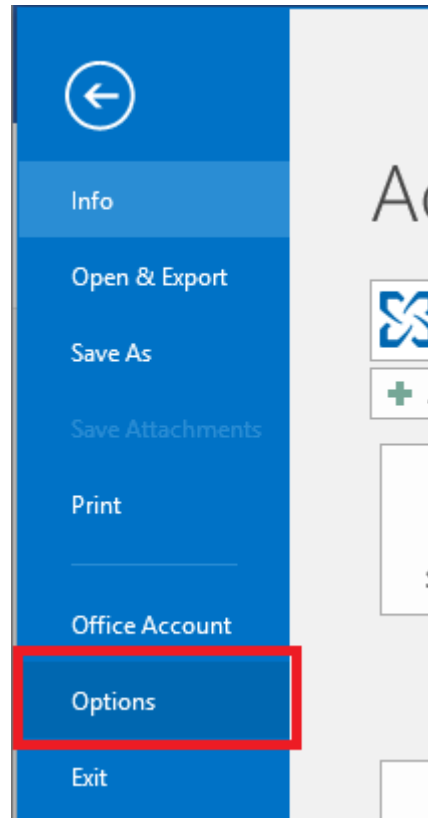All instructions below assume Windows 10 and Office 2016/Office 365
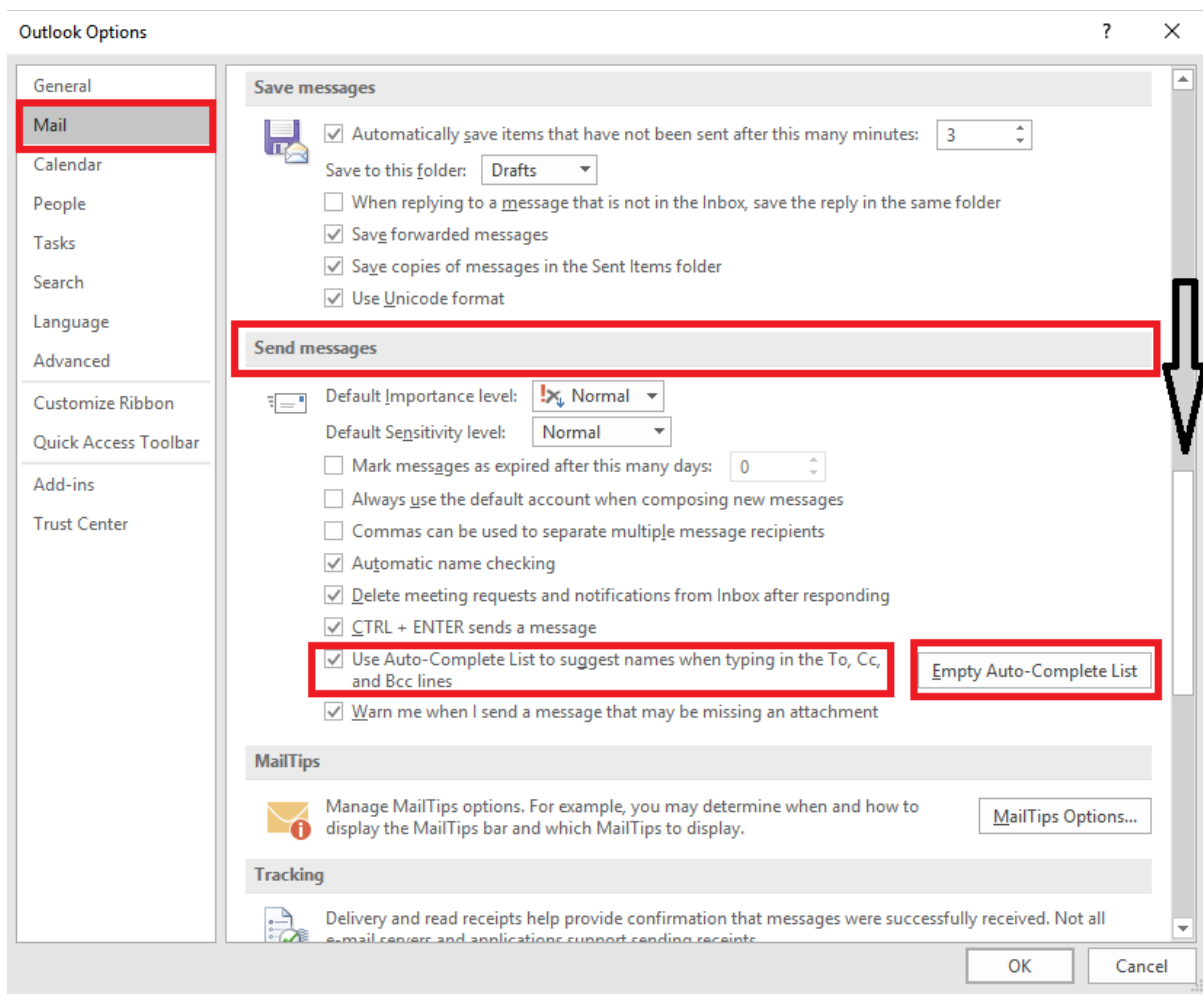
Appendix One

Disabling Auto Complete

To turn off the auto complete, click on the "File" Menu Option in Outlook

From the menu click on "Options"

From the "Outlook Options" window, click on "Mail" from the left hand list of options. Scroll down to the "Send Messages" section


Untick "Use Auto-Complete List to suggest names when typing in the To, CC and Bcc lines". Click the "Empty Auto-Complete List" to remove any already saved auto complete email addresses.

Click "OK" to save the changes. Auto Complete is now disabled.

Appendix Two

Password protecting a Word Document

To Encrypt and password protect a single Word document, click the "File" menu option in Word.
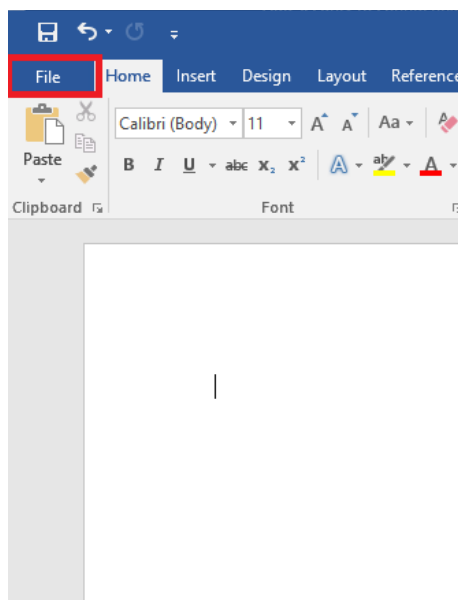
From the "File" Menu, Click the "Protect Document" box, click on "Encrypt with Password".
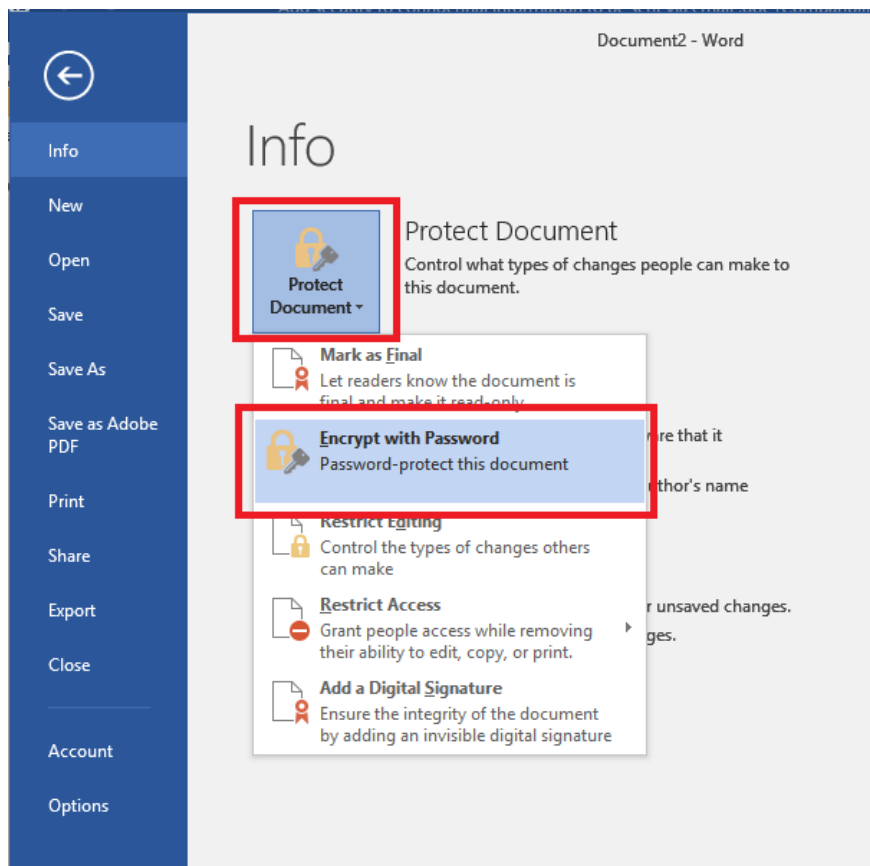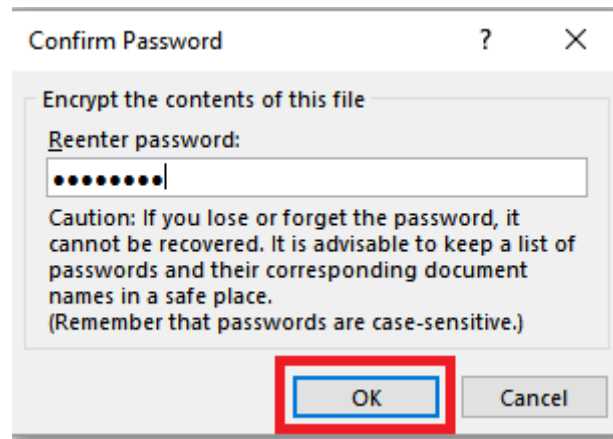
From the "Encrypt Document" window, type the password to be used.

Recommendation is that the password meets the following criteria;

- Minimum 10 characters
- Mix of upper case and lower case
- Contains at least one number
- Contains at least one special character (!,@,&,%,£ etc)
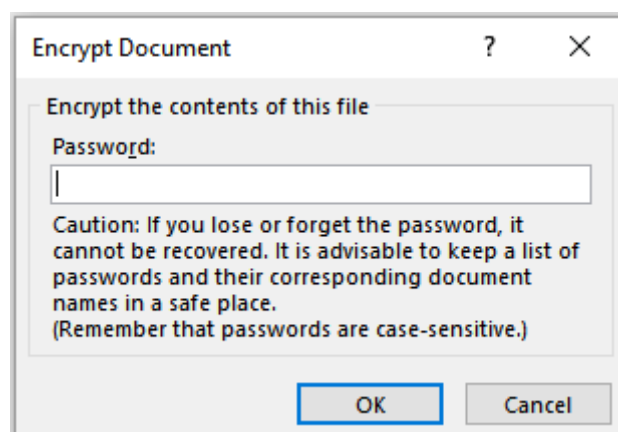
From the "Confirm Password" window, retype the same password, click OK to set the password.

Note: Word documents encrypted in the Universities Standard version of Office (2016) will be compatible with Word all version of Word back to version 2003. If the recipient has any difficulty opening an encrypted word document considerer using the instructions in Appendix 3, do not be tempted to send the Word Document unencrypted.

Appendix Three

Password protect documents when sending non Word or multiple documents.

Where multiple documents or files need to be emailed together encryption can be applied to all the files using one of the following solutions (depending on the age of the computer you will have one of the following programs installed)

- PeaZip
- 7zip

To determine which program is installed on the computer, right click on any document or file from any location on the computer. From the menu that appears you will see either; Peazip or 7zip in the menu.

Skip to the relevant instructions below Peazip or 7Zip

Note files created in either Peazip and 7zip are compatible with each other, they are also compatible with Winzip which is a paid version.

Peazip

Documents to be encrypted will need to be located on the local PC or R: drive not on One Drive or Tundra.

Once the Documents are copied to the computer, select all the documents to be encrypted (CTRL + A to select all or hold CTRL and left click on each files using the mouse)
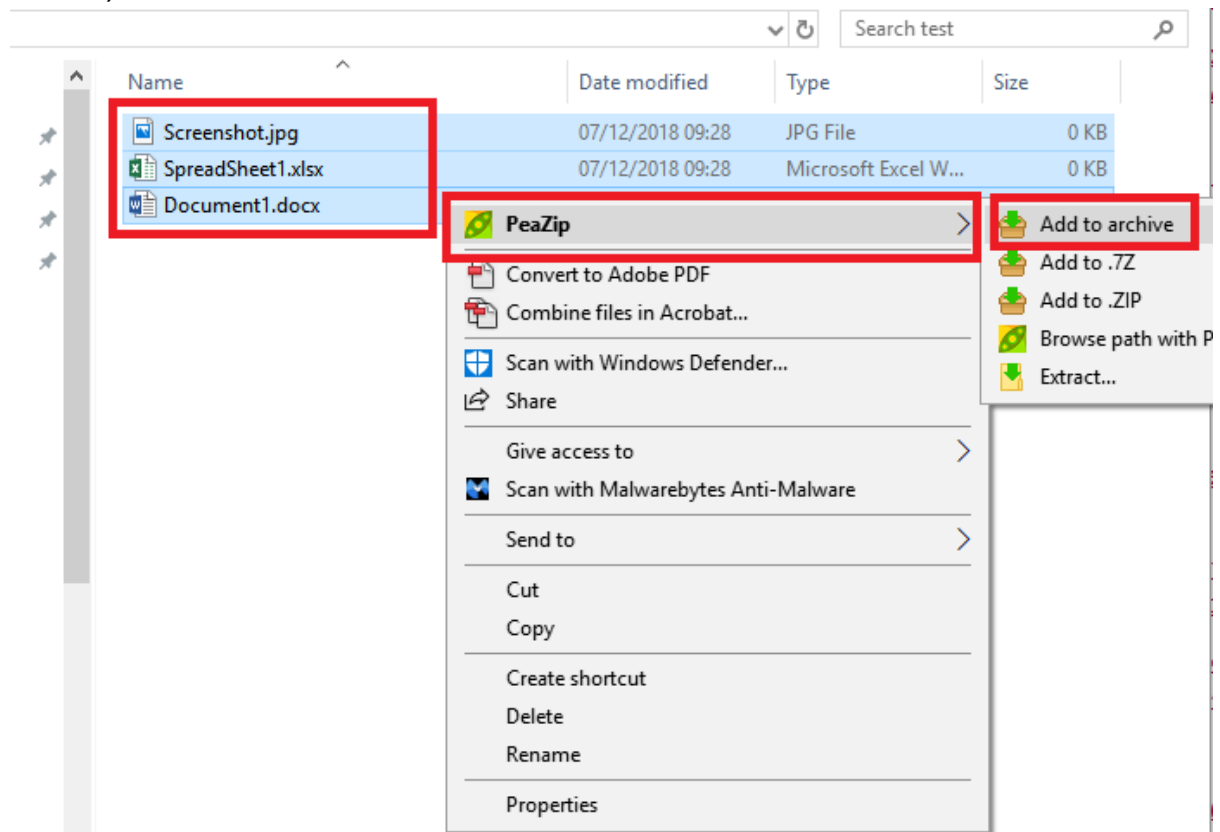
Right click on one of the documents to display the context menu

From the Context menu, move the mouse cursor over PEAZIP, to show an additional menu of Peazip options, click on "Add to Archive".

Peazip will open displaying a list of documents selected previously, from the drop downs select the following options;
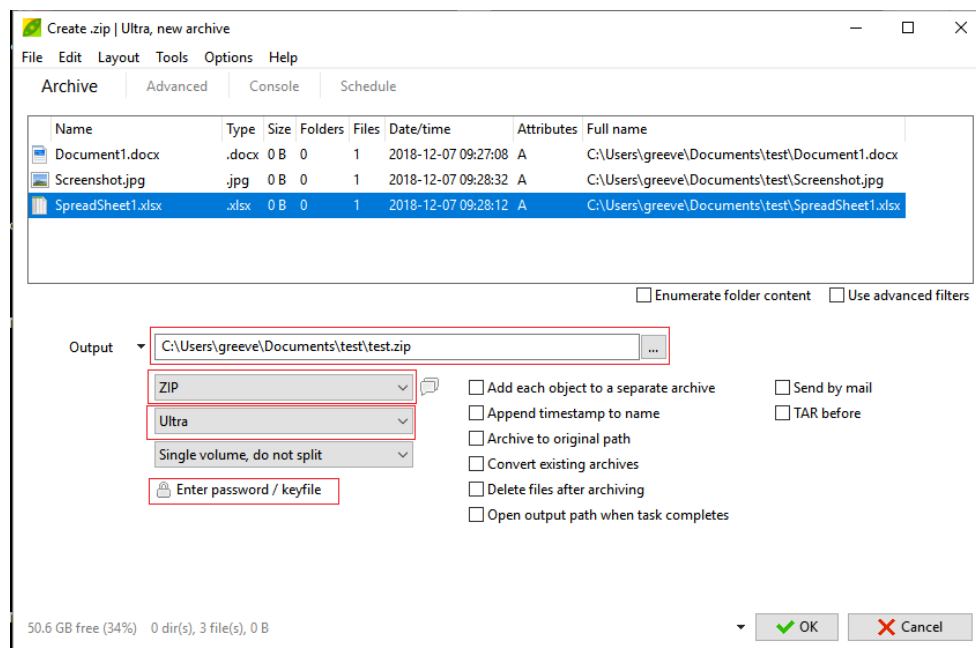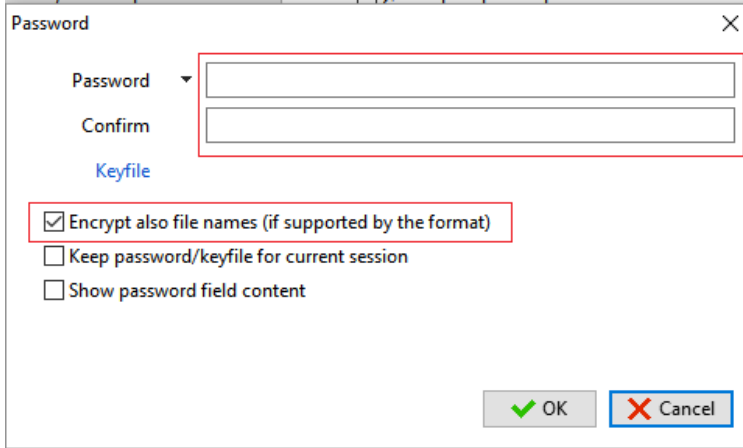
"Output"   Enter a meaningful file name at the end of the folder path <meaningfullname.zip>

From the drop down below "output" the two supported option are ZIP or 7z, either is acceptable, the recipient may have a preference both option are compatible with each other

From the next drop down, select "ULTRA" this will ensure the file created is a small as possible and will not cause delays when being emailed.

To set the password, click "Enter password/ keyfile".

In the Password menu enter a password. Passwords must be 10 characters' mix of upper lower case and at least one number and one special character

 DO NOT REUSE THE SAME PASSWORDS FOR DIFFERENT RECIPIENTS

Ensure that "Encrypt also file names (if supported by the format)" is ticked

Click OK to save the password and return to the main screen.

When a password has been entered the padlock icon next to the "Enter password / keyfile" option will show in yellow instead of grey, confirming a password has been set.

Click OK from the bottom right of the menu to create the encrypted file. Depending on how many documents have been selected and the speed of the computer this may take a minute to complete.
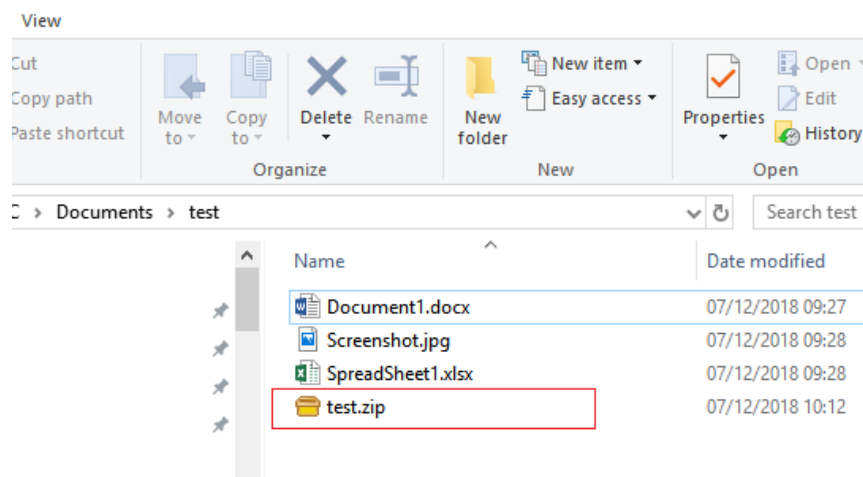

The encrypted file has been created, example shows as test.zip and contains all the required documents and files.

The encrypted file can now be sent via email

7Zip

Documents to be encrypted will need to be located on the local PC or R: drive not on One Drive or Tundra.

Once the Documents are copied to the computer, select all the documents to be encrypted (CTRL + A to select all or hold CTRL and left click on each files using the mouse)
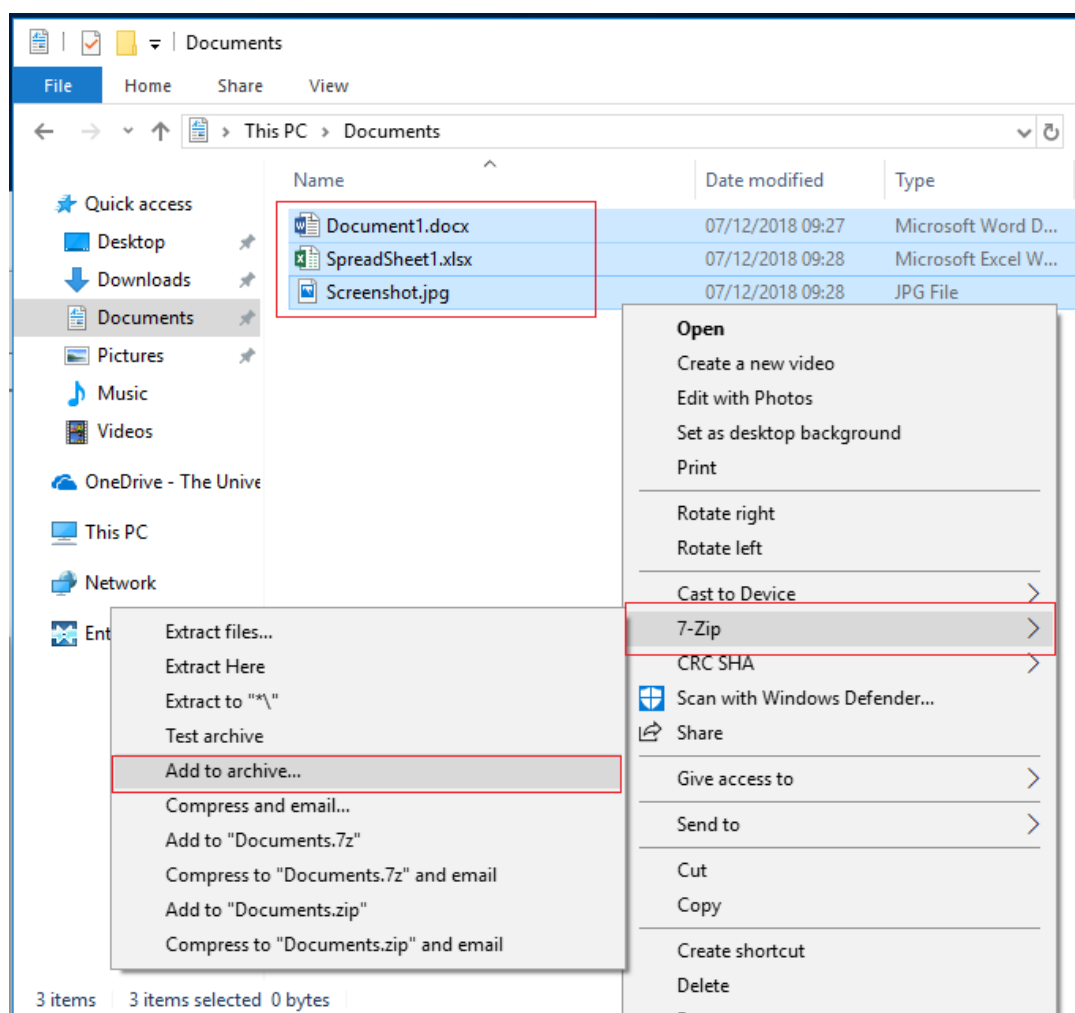
Right click on one of the documents to display the context menu

From the Context menu, move the mouse cursor over 7-zip, to show an additional menu of 7-Zip options, click on "Add to archive...".

In the "Archive:" field type a meaningful name for the encrypted file <meaningfullname.7z>

From the "Archive format" drop down select either 7z or ZIP as the only two support formats. Either is fine and both are compatible with each other.

From the "Compression level" drop down, select "ULTRA" this will ensure the file created is a small as possible and will not cause delays when being emailed.

In the "Encryption" section type the password and re-enter the same password.

Passwords must be 10 characters' mix of upper lower case and at least one number and one special character

DO NOT REUSE THE SAME PASSWORDS FOR DIFFERENT RECIPIENTS

Ensure the "Encryption Method" is set to AES-256.

Tick the "Encrypt File Names", click OK to create the encrypted file.

Depending on how many documents have been selected and the speed of the computer this may take a minute to complete.
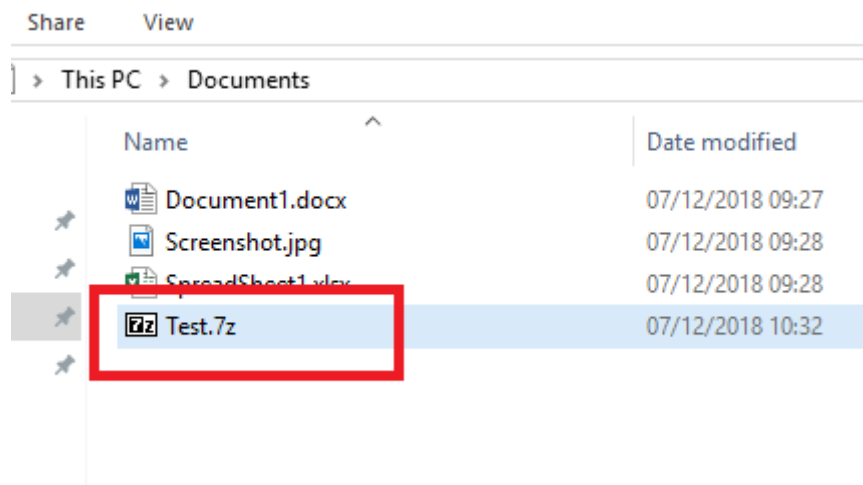
The encrypted file has been created, example shows as test.7z and contains all the required documents and files.

The encrypted file can now be sent via email