Ad hoc and manual transfer of sensitive data

If you regularly transfer sensitive data, contact servicedesk@abdn.ac.uk to discuss best methods for this.

Storage of sensitive data

Sensitive data *must be encrypted* before leaving the University, whether on physical media or electronically.

Physical media

Make sure any physical media you use for transfer, such as pen drive or external hard drive, is encrypted. For more information about encryption on Windows PCs, see our Bitlocker Fact Sheet. Macs have built-in encryption options.

Electronic transfer

ZendTo

Where you need to transfer data electronically, we recommend you use the University's **ZendTo** service (https://zendto.abdn.ac.uk/).

Files are automatically encrypted during transfer and you will receive notification when the recipient has picked up the file.

For particularly sensitive data, you should encrypt files first, before sending them with ZendTo.

You can send files up to 20GB in size.

Note: When using ZendTo, it is particularly important that you **type the recipient's email address correctly** to ensure files are delivered to the correct person.

Email

You can also use email to transfer sensitive data but you **must** encrypt files **before** sending.

The maximum attachment file size is 150Mb and there are restrictions on file types that can be sent as attachments.

Methods of encryption of files before electronic transfer (Windows)

There are two recommended methods of encrypting files before sending using utilities installed on University managed Windows PCs.

1. **Office 365** (with the default AES-256 encryption).
   This is the simplest method if a single Office file is to be transferred and it is accepted by most email systems.

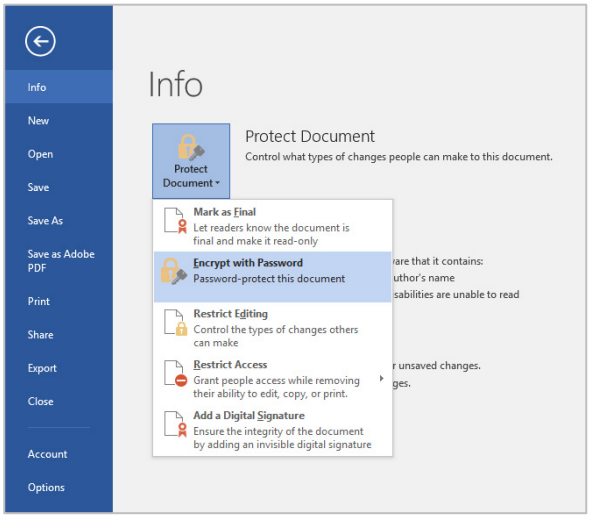
2. **7-Zip**
   This method is best for encrypting a number of files at once, or for a non-Office document. However, the resulting **zip** files are **not** usually accepted by email systems (this includes email coming into the University of Aberdeen with zip attachments).

   Note: In order to decrypt and open files encrypted in this way, recipients must also have the relevant software, i.e. Office 365 or 7-Zip.

Method 1 – Office 365

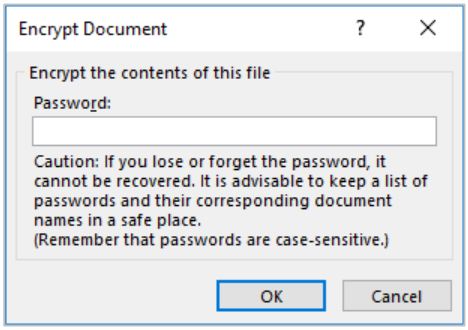
- **Open** the Word file
- From the **File** menu, select **Info**
- Click the drop-down menu **Protect Document**
- Select **Encrypt with Password**

  Note: For an Excel file this will be **Protect Workbook**, and for a PowerPoint file, **Protect Presentation.**



- **Enter** a password and re-enter when prompted. See Password Advice below.
- Click **OK**

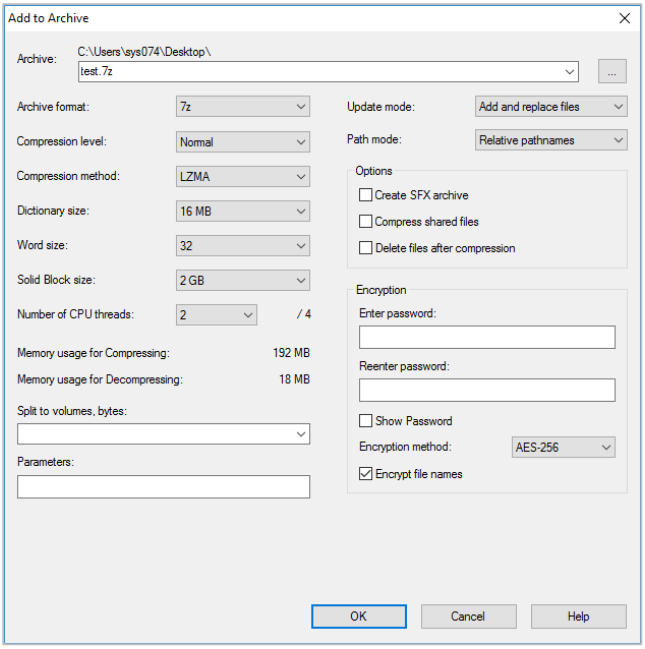
  Note: If you want to add more files you must create a new archive, otherwise your added files may not be encrypted.



Method 2 – 7-Zip

- **Locate** the file or folder you want to encrypt
- **Right click** on it
- Choose **7-Zip** and then **Add to archive…**
- Ensure you **select**:
  - Archive Format: **7z**
  - Encryption Method: **AES-256**
  - Encrypt file names: **ticked**
- **Enter** a password and re-enter. See Password Advice below.
- Click **OK**

  Note: If you want to add more files you must create a new archive, otherwise your added files may not be encrypted



Password Advice

- The password you choose to encrypt files **must** be complex (64 random hexadecimal characters recommended see: https://www.grc.com/passwords.htm).
- Simple dictionary words should not be used as they are too easy to crack.
- Passwords should not be emailed to the recipient.

  Alternative methods of passing on the password include: text message, phone call or physical letter. If this is not practical, the password may be emailed but should be in a separate email message from the encrypted file.
- **Confirm** that your intended recipient has received the password before sending the encrypted file by email or ZendTo transfer. This is to ensure that there have not been any errors in the email address you entered.

Further information and help

If you any require further assistance, please contact the IT Service Desk – https://myit.abdn.ac.uk