Information Security: Transfer of sensitive data

Note: This guidance is intended for those who transfer sensitive, personal, or confidential data manually on an ad hoc basis.

If you *regularly* transfer such data, contact the IT Service Desk servicedesk@abdn.ac.uk to discuss best methods for this.

Encryption of sensitive, personal, or confidential data

Sensitive, personal, or confidential 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 Encryption Guide. Macs have built-in encryption options.

Electronic transfer

ZendTo

Where you need to transfer files that contain sensitive, personal, or confidential data electronically, we recommend you use the University's **ZendTo** service (https://zendto.abdn.ac.uk/) and that you encrypt the files using 7-Zip before uploading them.

If you are going to send files that contain sensitive, personal, or confidential data to colleagues *outwith* the University, **it is *mandatory* to first encrypt the files using 7-Zip *before* uploading to ZendTo.**

Find out more about using ZendTo to securely send files that contain sensitive, personal, or confidential data, in our dedicated user guide.

Email

If you intend to use email to transfer sensitive, personal, or confidential data, **you must encrypt files before sending**.

Note that the maximum attachment file size is 35Mb and there are restrictions on file types that can be sent as attachments. Use ZendTo as an alternative if required.

Methods of file encryption before electronic transfer (Windows)

There are two recommended methods of encrypting files before sending using utilities installed on University managed Windows PCs – **7-Zip** and **Office 365**. These are described below.

Note: In order to decrypt and open files that have been encrypted using either of these method, recipients must also have the relevant software, i.e. 7-Zip or Office 365.

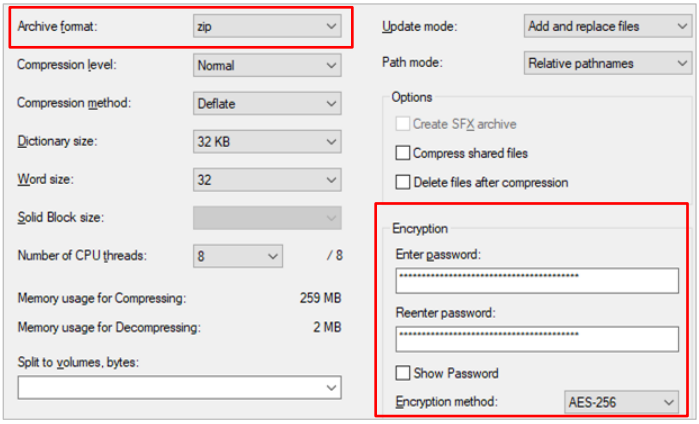
Method 1: 7-Zip

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

7-Zip is FREE software installed by default on managed University of Aberdeen desktops and laptops. If you cannot find it on your University computer then you can install it via Software Center.

You can also download a copy to a personal computer from https://www.7-zip.org/download.html.

1. **Locate** the file or folder you want to encrypt and **right click** on it.
2. From the pop-up menu, choose **7-Zip > Add to archive...**
3. In the Add to Archive dialog:
   - Archive Format: **zip**
   - Encryption Method: **AES-256**

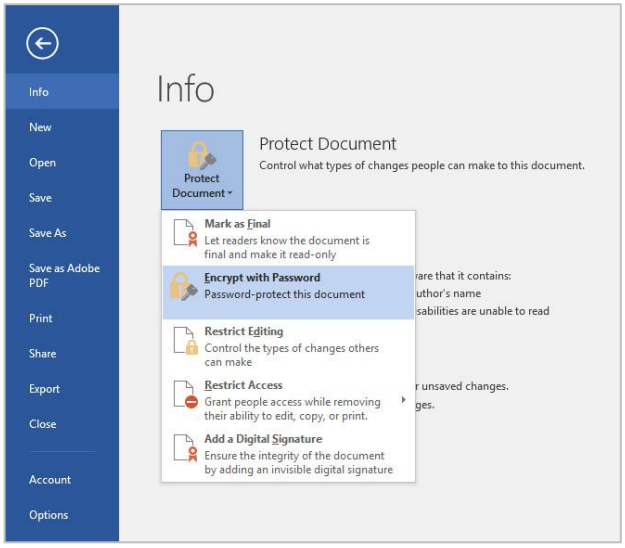


4. **Enter** a password, then reenter it.
   - For **Password Advice**, see below.
   - Make a note of the password as you will send it to your colleague separately.
5. Click **OK**
   - **Note:** If you want to add more files you must create a new archive, otherwise your added files may not be encrypted

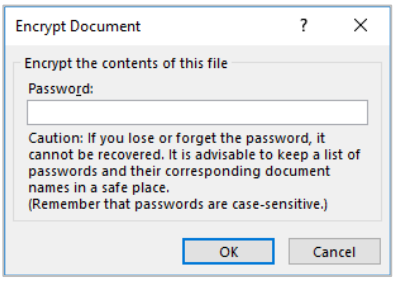
Method 2: Office 365 (with the default AES-256 encryption).

This is the simplest method if you need to transfer a single Office file, and it is accepted by most email systems.

1. **Open** the Office file, e.g. Word.
2. From the File menu, select **Info**.
3. Click the **Protect Document** drop-down menu.
   - For an Excel file this will be **Protect Workbook**.
   - For a PowerPoint file this will be **Protect Presentation**.
4. Select **Encrypt with Password**.



5. Enter a password and re-enter it when prompted.
    - For **Password Advice**, see below.
    - Make a note of the password as you will send it to your colleague separately.
6. 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

- Your password must be complex (containing at least 8 random characters, including a mix or upper and lower case, numeric, and special characters) and should not be a dictionary word.
- Ideally, 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 ZendTo or email transfer. This is to ensure that there have not been any errors in the email address you entered.

Further information and help

If you need further guidance on the secure transfer of sensitive data, please contact the Information Governance Team at dpa@abdn.ac.uk.