Data Protection Protocols

Key Messages

- The data protection protocols are designed as guidance for DPCs and other members of staff who require relevant assistance.
- The protocols provide guidance and best practice around key data protection & information security aspects of UWE's business.
- The guidance provided should always be considered and applied where appropriate.
- If you are still unsure, please contact the Data Protection Office.
- If you have any further suggestions for this or any other protocol, please contact the Data Protection Office.

Protocol [4]: Encryption

1.1. What is encryption

Encryption is the term often used to describe the process of ensuring that important, sensitive or personal data is appropriately secured. It applies to data whilst in transit i.e. when being sent and received across a network and whilst also at rest, i.e. in storage.

The process works by converting data using a secret code into an unrecognisable, or 'encrypted' format. This means that unless you have the code key, you will be unable to read the information.

1.2. Why are we using encryption and its associated benefits?

- Encryption protects customers and staff from harm caused by failure to keep UWE data confidential and secure
- It protects data against unauthorised access if the device storing the encrypted data is lost or stolen.
- Encryption is a means by which we can demonstrate compliance with the security requirements of the GDPR.
- If the security aspects of password keys are effectively managed then encrypting data whilst it is being stored (e.g. on a laptop, mobile, USB or back-up media, databases and file servers) provide effective protection against unauthorised or unlawful processing.
- In terms of GDPR, appropriate encryption methods are seen as a good security practice designed to safeguard personal data.

1.3. What is the UWE 'Information Handling Policy' document?

The purpose of this policy is to seek to ensure staff and students understand how information in their possession should be protected, and how information should be shared with other parties. It is important to recognise that different types of information require specific security measures, and therefore proper classification of information assets is vital to ensure effective information security and management practices are adhered to across the University. The UWE Information Handling Policy document forms part of the Information Security Policy Toolkit and underpins the overarching Information Security Policy. Adherence to this policy will provide everyone with guidance to help ensure that correct information classification and handling methods are applied to their day-to-day activities and managed accordingly.

1.4. When and how to use it?

Before you send anything that contains personal data you will should consider if you really need to send the information? If the answer is 'No' then you should not send it. If the answer is 'Yes' then you will need to ensure you are doing so in a safe and secure manner and one which conforms to the requirements of GDPR.

If you have to share personal data then the most secure way of doing so is to always send a link to your document from Sharepoint or One Drive. This will ensure that only authorised individuals will be able to access it. For further information please refer to – UWE Information Security Toolkit – Secure Storage.

If this cannot be performed then you should refer to one of the use cases listed below for further guidance:

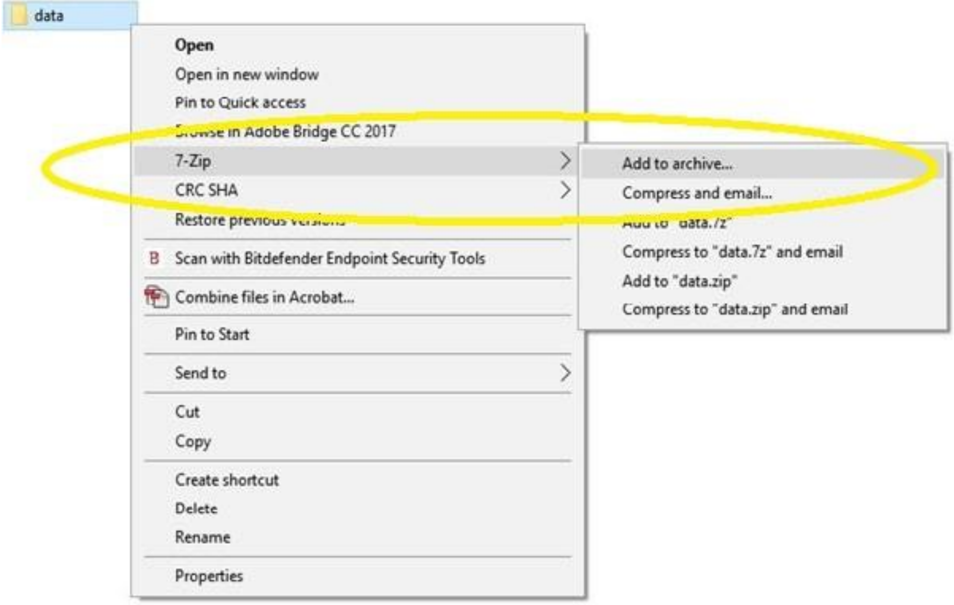
Use Case	**Please Refer to:**
If you are using a UWE/Non-UWE owned Windows device and you need to encrypt any files or folders containing UWE personal data including PDF files.	Appendix A: Encrypt Using 7-Zip (Windows)
If you are using a UWE/Non-UWE owned Mac device and you need to encrypt any files or folders containing UWE personal data including PDF files.	Appendix B: Encrypt Using 7-Zip Equivalent (Mac)
If you are trying to encrypt a USB device on a UWE/Non-UWE owned Windows device.	Appendix C: USB Stick Encryption (Windows)
If you are trying to encrypt a USB device on a UWE/Non-UWE owned Mac device.	Appendix D: USB Stick Encryption (Mac)
If you are trying to password protect Microsoft Office documents on a UWE/Non-UWE owned Windows device.	Appendix E: Password protect Microsoft Office documents (Windows)
If you are trying to password protect Microsoft Office documents on a UWE/Non-UWE owned Mac device.	Appendix F: Password protect Microsoft Office documents (Mac)
If you are trying to perform access restrictions on Microsoft Office documents on a UWE/Non-UWE owned Windows device.	Appendix G: Restrict Access to Microsoft files and document (Windows)

If you are trying to perform device encryption on a UWE/Non-UWE owned Windows device.	Appendix H: Device Encryption (Windows)
If you are trying to perform device encryption on a UWE/Non-UWE owned Mac device.	Appendix I: Device Encryption (Mac)
For anything else not listed	Appendix J: Further Information:

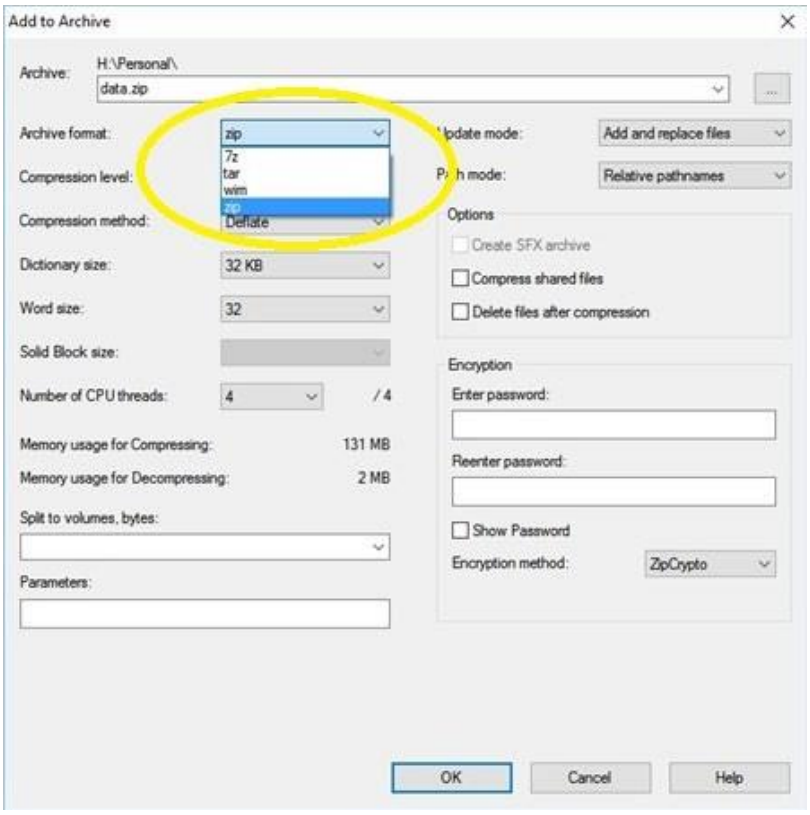
Appendix A: Encrypt Using 7-Zip (Windows)

In order to encrypt documents and folders using 7-Zip you will need to perform the following:

To create the file, right click on the files or folders that you would like to encrypt, and select '7-Zip' > 'Add to archive'.



Enter the name you wish to give the file, and select '.zip' as an archive format.



Add to Archive

Archive: H:\Personal\ data.zip

Archive format: zip

Compression level:

Compression method: Deflate

Dictionary size: 32 KB

Word size: 32

Solid Block size:

Number of CPU threads: 4 / 4

Memory usage for Compressing: 131 MB

Memory usage for Decompressing: 2 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

Path mode: Relative pathnames

Options

□ Create SFX archive

□ Compress shared files

□ Delete files after compression

Encryption

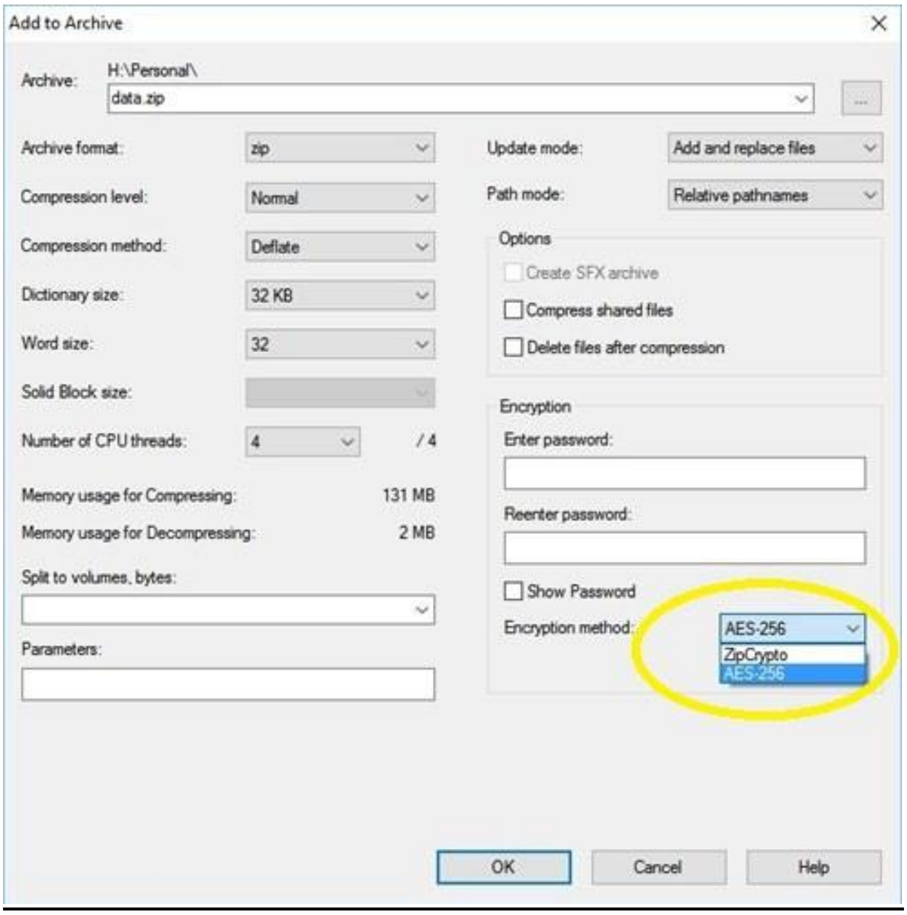
Enter password:

Reenter password:

□ Show Password

Encryption method: ZipCrypto

Make sure that the Encryption method is set to ‘AES-256’ - this method is more secure than ZipCrypto (the default).



Add to Archive

Archive: H:\Personal\ data.zip

Archive format: zip

Compression level: Normal

Compression method: Deflate

Dictionary size: 32 KB

Word size: 32

Solid Block size:

Number of CPU threads: 4 / 4

Memory usage for Compressing: 131 MB

Memory usage for Decompressing: 2 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

Path mode: Relative pathnames

Options

□ Create SFX archive

□ Compress shared files

□ Delete files after compression

Encryption

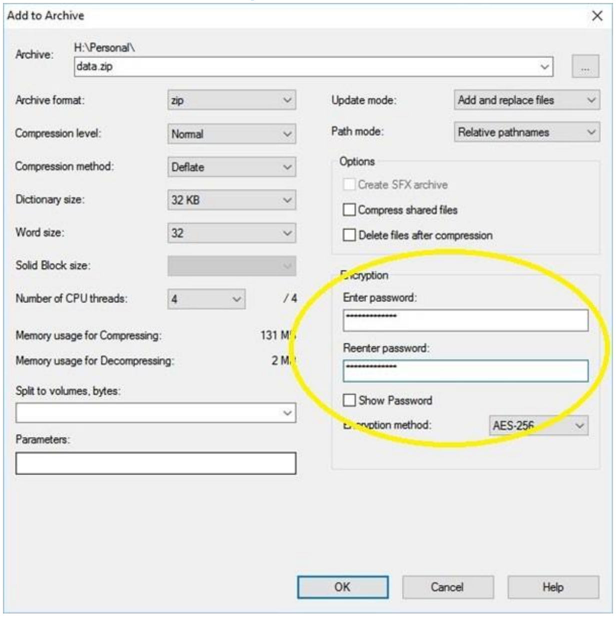
Enter password:

Reenter password:

□ Show Password

Encryption method: AES-256

Enter a password of your choice in the Encryption/highlighted section below. The password will be needed to open files. To ensure your data is properly protected, choose a strong password. Further guidance on creating strong passwords can be found at - [UWE - Information Security Toolkit - Passwords]().



Add to Archive

Archive: H:\Personal\ data.zip

Archive format: zip

Compression level: Normal

Compression method: Deflate

Dictionary size: 32 KB

Word size: 32

Solid Block size:

Number of CPU threads: 4 / 4

Memory usage for Compressing: 131 MB

Memory usage for Decompressing: 2 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

Path mode: Relative pathnames

Options

□ Create SFX archive

□ Compress shared files

□ Delete files after compression

Encryption

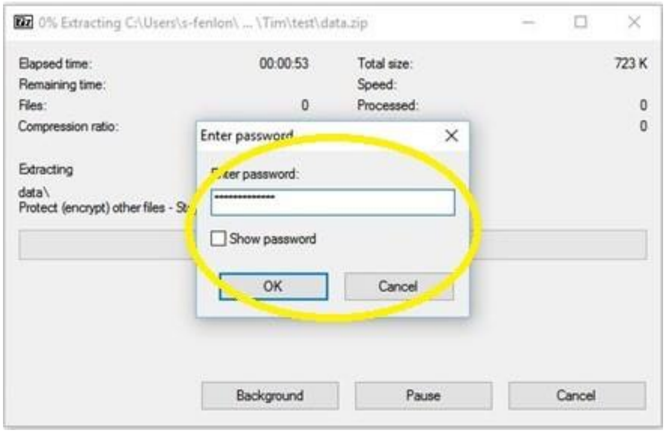
Enter password: **************

Reenter password: **************

□ Show Password

Encryption method: AES-256

Enter the password to open your files (Please note that when encrypting a zip file, only the contents of the files within the archive are protected. File names and directory listings are visible to users without the password).



0% Extracting C:\Users\s-fenlon\ ... \Tim\test\data.zip

Elapsed time: 00:00:53
Remaining time:
Files: 0
Compression ratio:
Total size: 723 K
Speed:
Processed: 0
0

Extracting
data\
Protect (encrypt) other files - St

Enter password
Enter password: **************
□ Show password

Importantly, please remember the following information:

- Share the password using a different method to the way you share the file i.e. by using Skype, by telephone or in person;
- Share the password with the minimum number of people necessary;
- Retain encrypted documents and files only for as long as necessary;
- Ensure encrypted document, files and folders are appropriately deleted when no longer necessary;
- Do not create unencrypted copies of your documents, files and folders.

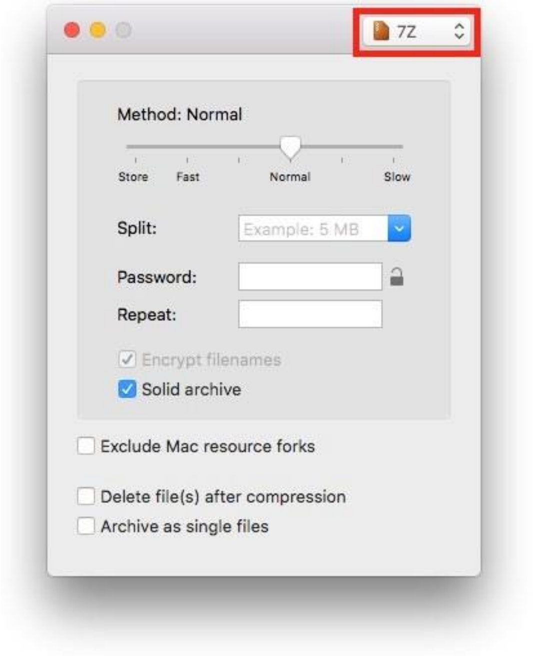
Further information can be found at - **UWE - Information Security Toolkit - 7-Zip**

Appendix B: Encrypt Using Keka (Mac)

A Mac alternative to 7-Zip is a free application called Keka - https://www.keka.io/en/

If you have a business requirement to share personal information you will need to encrypt your files or folders. Keka can perform this as shown below. Using a .ZIP format, input the desired password in the "Password" and "Repeat" fields, the padlock will close, and you're set.

1) Once opened, from the top right menu, select 'ZIP'



Method: Normal

Split: Example: 5 MB

Password:

Repeat:

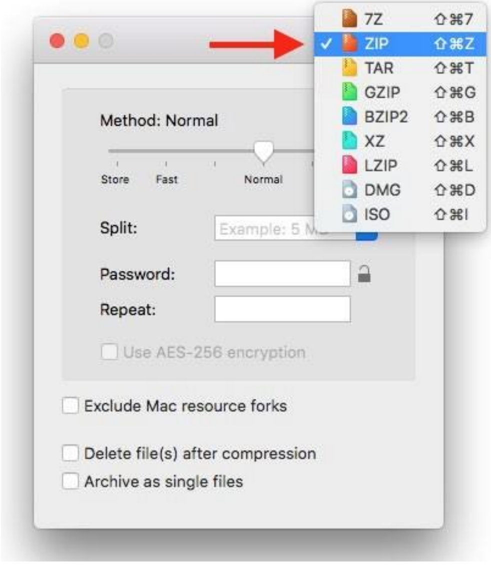
☑ Encrypt filenames

☑ Solid archive

□ Exclude Mac resource forks

□ Delete file(s) after compression

□ Archive as single files



Method: Normal

Split: Example: 5 M

Password:

Repeat:

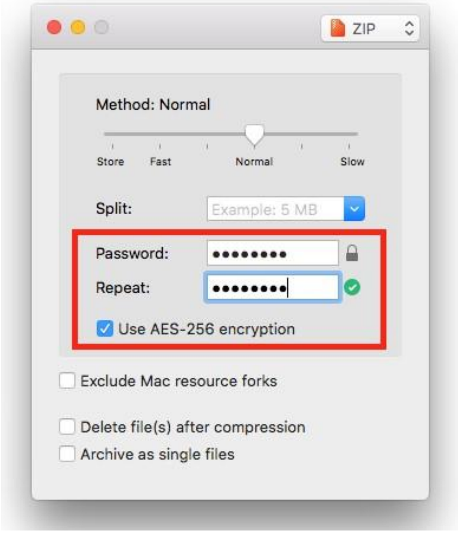
□ Use AES-256 encryption

□ Exclude Mac resource forks

□ Delete file(s) after compression

□ Archive as single files

2) Enter a suitably strong password and tick ‘Use AES-256 encryption'



ZIP

Method: Normal

Split: Example: 5 MB

Password: ••••••••

Repeat: ••••••••

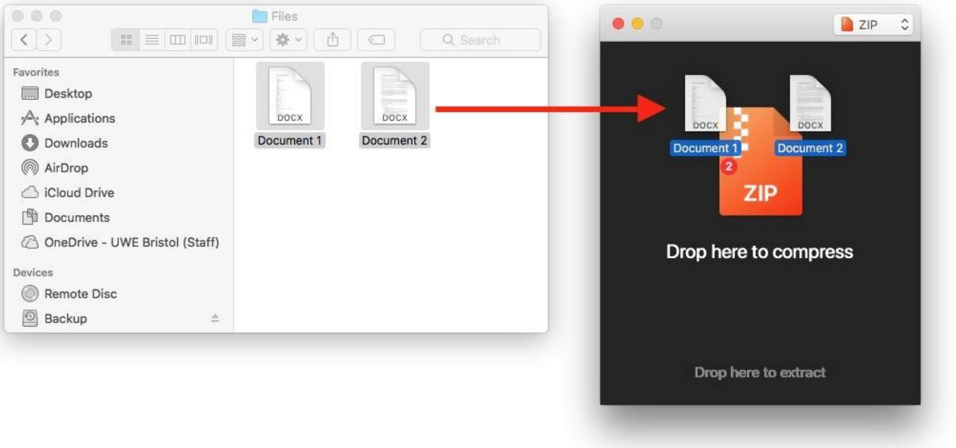
☑ Use AES-256 encryption

□ Exclude Mac resource forks

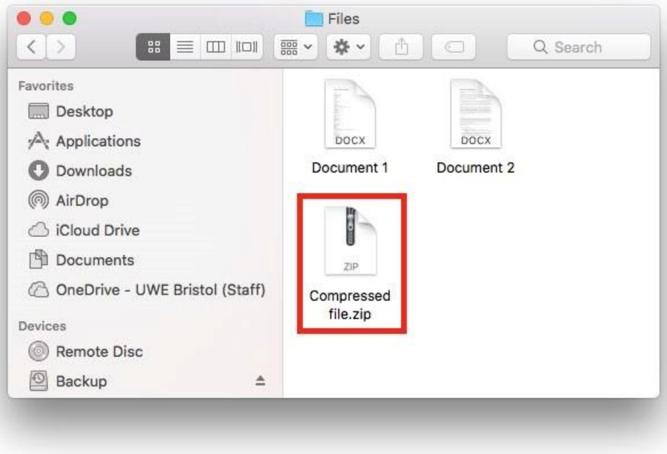
□ Delete file(s) after compression

□ Archive as single files

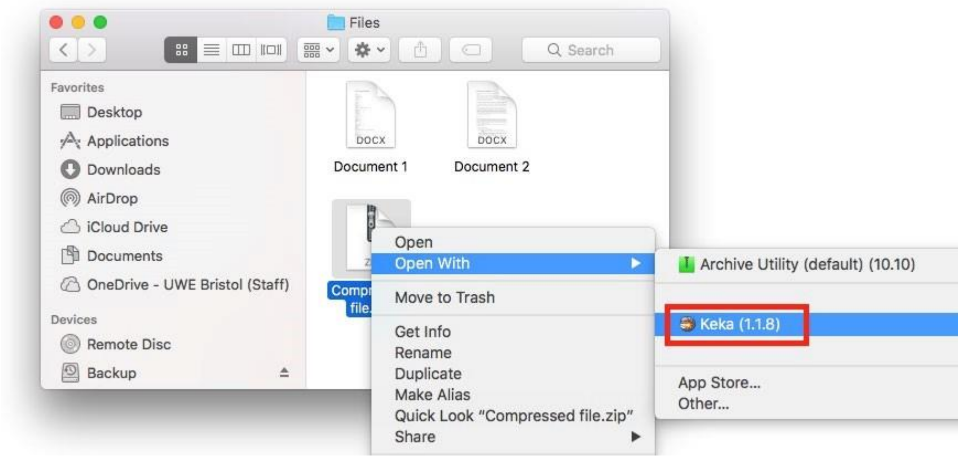
3) Drag the file(s) or folder(s) you want to zip onto the main Keka window.



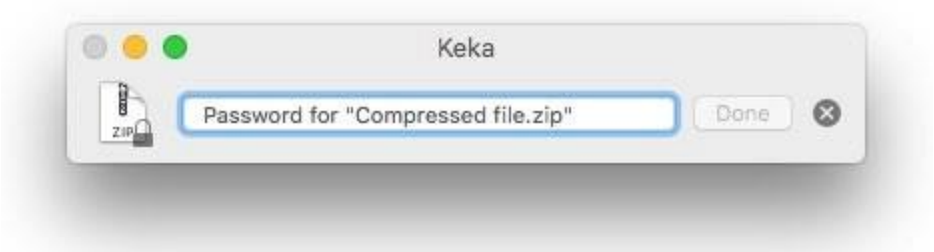
4) Keka will then create the zipped file in the same folder as your original files.



5) To open the zip file, it’s necessary to right click, then select ‘Open With’ -> ‘Keka’.



6) Enter the password, then click done.



UWE acknowledges that as part of its working practices and processes, its partners and third parties may require an understanding of encryption tools, in particular Keka.

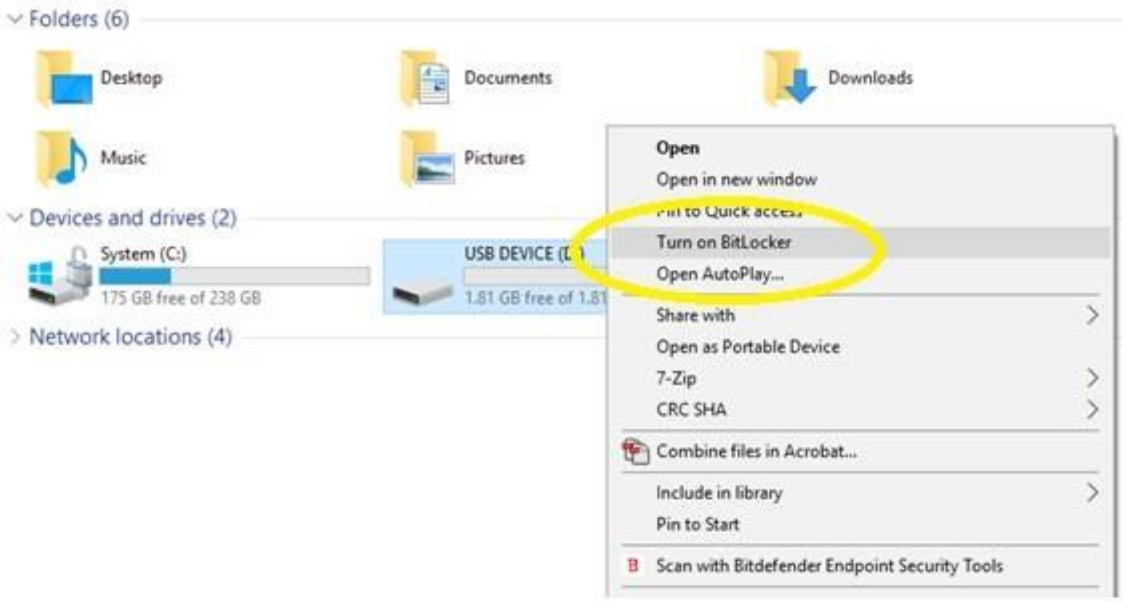
Keka is a free download for both personal use and commercial organisations. It can be downloaded from the main Keka site: https://www.keka.io/en/

Please note that .ZIP files, encrypted with Keka, can also be shared with Windows devices and unencrypted using WinZip.

This is also true for .7z files, encrypted with 7-Zip, that can be shared with Mac users and unencrypted using Keka.

Appendix C: USB Stick Encryption (Windows)

When working with USB devices* and personal/sensitive information you have two options. You can either use BitLocker to encrypt the entire device:



Or, alternatively, you could encrypt your individual documents and folders using 7-Zip, this would not need to go on an encrypted USB device.

An encrypted USB device can be decrypted using any other Windows device - even if it was originally encrypted using a UWE device. You will, however, be expected to enter the encryption key/password as part of the unencryption process.

***The term USB device includes memory sticks, flash drives, pen/thumb drives and external hard drives – Furthermore, you will also need to ensure that you have processes in place for managing such devices securely. Whilst out of scope for this document, as part of this process you should consider:**

- **Allocating device owners;**
- **How these devices will be stored securely;**
- **Regular Auditing**

Please note that Windows 7, 8 and 10 Home versions have no BitLocker functionality. However, you will still be able to decrypt BitLocker encrypted devices using Windows own built in tools.

Remember, that you should not be connecting any unknown USB drives to any computer, specifically UWE devices.

Appendix D: USB Stick Encryption (Mac)

Encrypting a portable USB* drive is a great way to prevent sensitive data falling into the wrong hands, preventing data breaches and security incidents. This guide will demonstrate how to securely encrypt a USB flash drive within macOS so that the data stored on it cannot be read nor accessed without entering a secure password.

***The term USB device includes memory sticks, flash drives, pen/thumb drives and external hard drives – Furthermore, you will also need to ensure that you have processes in place for managing such devices securely. Whilst out of scope for this document, as part of this process you should consider:**

- **Allocating device owners;**
- **How these devices will be stored securely;**
- **Regular Auditing**

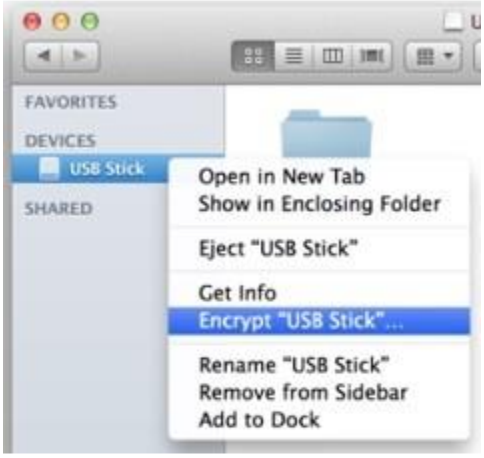
Requirements

This guide applies to encrypting a flash drive on macOS El Capitan and Sierra using the built in encryption tool known as FileVault:

- Drives encrypted with FileVault CANNOT be opened by Windows.
- The password you choose to protect your USB flash drive CANNOT be changed once it is configured.

Follow the steps below to encrypt a USB flash drive using macOS.

1. Insert your USB flash drive into your Mac.
2. When the icon appears on your desktop, right click on it and select Encrypt.



3. You will then need to enter and confirm a password (as well as a password hint). This password CANNOT be changed. For guidance on strong passwords see UWE - Information Security Toolkit - Passwords
4. Encryption should only take a few minutes; once complete, you USB flash drive will be fully protected.

How to use your newly encrypted USB flash drive

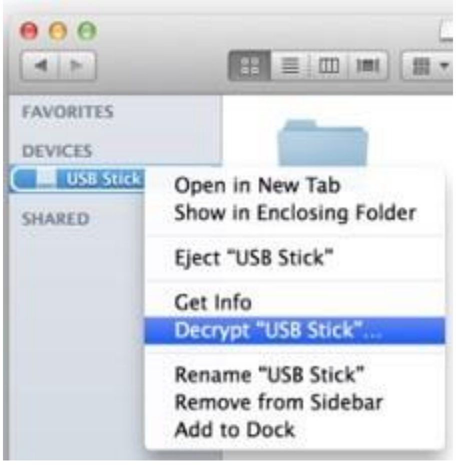
To securely use your encrypted USB flash drive, simply plug it into your computer. You will be prompted to enter the password you used to encrypt your drive.

Your macOS computer will automatically manage encrypting and decrypting your information while it is plugged in to your computer. When you are done working on your data, simply unplug it from your computer.

How to disable encryption

If you no longer wish to utilise encryption on your USB drive, you can permanently disable it. This action will remove the encryption and allow you to use the drive on computers that do not support FileVault, and will permanently stop securing the data on your USB drive.

To disable encryption, right-click on the drive in Finder and select Decrypt.

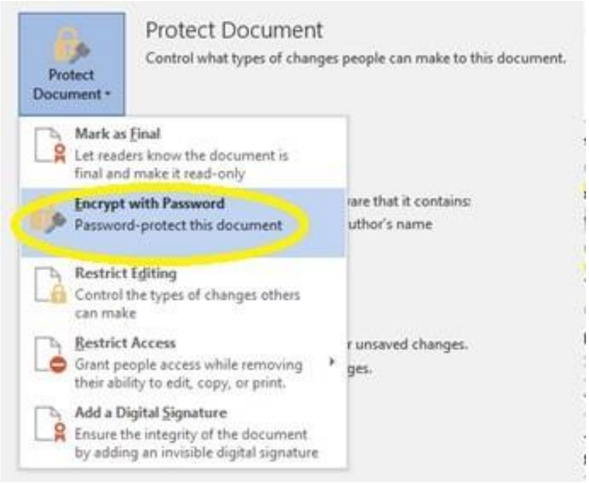


You will be prompted for your encryption password. Once you confirm your action, macOS will remove encryption from the USB flash drive; this action will take some time. Once complete, you can remove your USB flash drive and use it normally without restriction.

Appendix E: Password protect Microsoft Office documents (Windows)

In order to password protect a Microsoft document then:

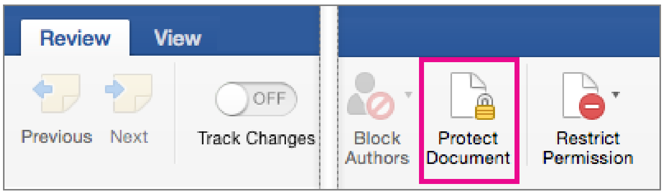
Left click "File" > "Info" > "Protect Document" > "Encrypt with Password". Enter a strong and memorable password. For guidance on strong passwords see UWE - Information Security Toolkit - Passwords


Protect Document
Protect Document
Control what types of changes people can make to this document.
Mark as Final
Let readers know the document is final and make it read-only
Encrypt with Password
Password-protect this document
Restrict Editing
Control the types of changes others can make
Restrict Access
Grant people access while removing their ability to edit, copy, or print.
Add a Digital Signature
Ensure the integrity of the document by adding an invisible digital signature
are that it contains:
uthor's name
r unsaved changes.
ges.

Appendix F: Password protect Microsoft Office documents (Mac)

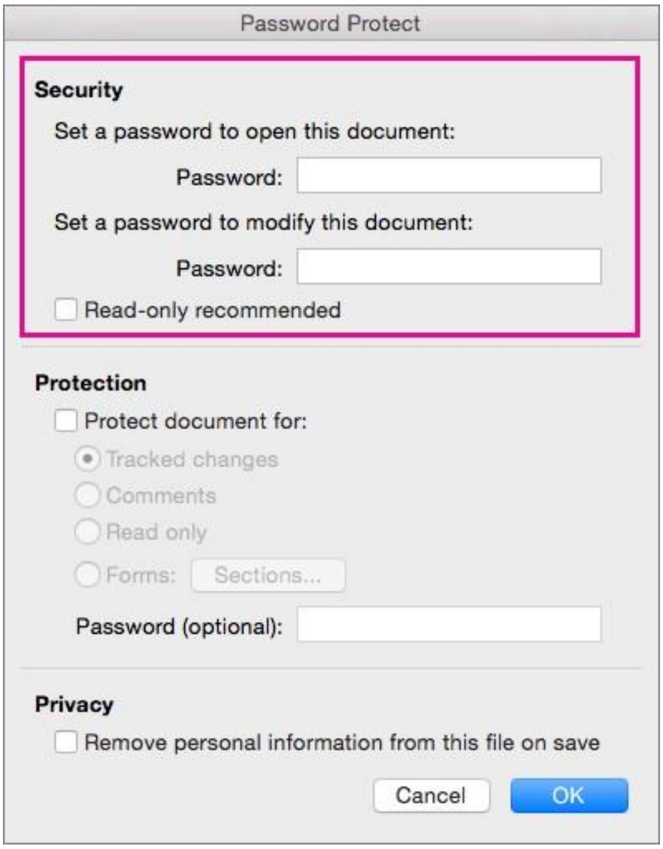
Protect your document from being opened or edited 1.

Click **Review** > **Protect Document**.



2. Under **Security**, you can select whether to enter a password to open the document, modify the document, or both. Enter each password again to confirm. For guidance on strong passwords see UWE - Information Security Toolkit - Passwords

Data Protection Protocols



Password Protect

Security

Set a password to open this document:

Password:

Set a password to modify this document:

Password:

□ Read-only recommended

Protection

□ Protect document for:

● Tracked changes

○ Comments

○ Read only

○ Forms: Sections...

Password (optional):

Privacy

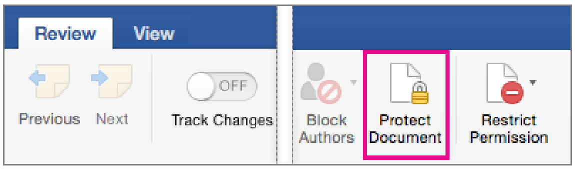
□ Remove personal information from this file on save

- Passwords are case-sensitive and can be a maximum of 15 characters long.
- If you lose or forget your password, Word won't be able to recover it for you. Be sure to keep a copy of the password in a safe place or create a strong password that you'll remember.

3. Click **OK**.

Protect your document before sending it out for review Click

Review > **Protect Document**.



1. Under **Protection**, select **Protect document for**.
2. Do one of the following.

To Do this:

Click **Tracked** Keep

Tracked Changes on.

changes

Allow people to add comments. Click **Comments**

Prevent people from making changes. Click **Read only**

Restrict changes to forms, so people can fill out the form
Click **Forms** without accidentally changing the form itself.

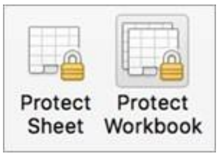
3. To prevent people from changing the protection settings, type a password in the **Password** box.
4. Click **OK** when you're finished.
5. **Note:** If you share a document with other people, you can remove personal information, such as author name and company, when you save a file. To do this, under **Privacy** at the bottom of the **Password Protect** dialog box, select **Remove personal information from this file on save**.

Require a password to open or modify a workbook

You can help prevent unauthorized users from opening or modifying a workbook file, even if they have permission to open it.

Caution: When you create a password for a workbook, write down the password and keep it in a secure place. If you lose the password, you can't open or gain access to the password-protected workbook.

1. Open the sheet or workbook that you want to protect.
2. On the **Review** tab, click **Protect Sheet** or **Protect Workbook**.



3. In the **Password** box, type a password, and in the **Verify** box, type the password again. For guidance on strong passwords see UWE - Information Security Toolkit - Passwords
4. Choose any other protection options you want and click **OK**.
5. Click **Save**.
6. **Tip:** To remove a password, click **Unprotect Sheet** or **Protect Workbook** and enter the password.

Password protect a presentation in PowerPoint for Mac

You can use passwords to help prevent other people from opening or modifying your presentations.

Caution: When you create a password for a presentation, record the password and keep it in a secure place. If you lose the password, it can't be retrieved and you won't be able open or gain access to the presentation.

Require a password to open a presentation

1. Click **File** > **Passwords**.
2. Under **Password to open**, select the **Encrypt this presentation and require a password to open** check box.
3. In the **New password** box, type a password.

   Note: To create a strong password, use at least seven characters and include a combination of uppercase and lowercase letters, numbers, and non-alphabetic characters such as !,$, #, and %. Do not include your account name or other personal information.

   For guidance on strong passwords see UWE - Information Security Toolkit - Passwords

4. In the **Verify** box, type the password again, and then click **Set Password**.
5. Click **OK**, and then save your presentation.

   Tip: To remove the password, clear the **Encrypt this presentation and require a password to open** check box, click **OK**, and then save your presentation.

Change a password to open or modify a presentation

1. Click **File** > **Passwords**.
2. Under **Password to open** or **Password to modify**, click **Change Password**.
3. In the **New password** box, type the new password.

   Note: To create a strong password, use at least seven characters and include a combination of uppercase and lowercase letters, numbers, and non-alphabetic characters such as !,$, #, and %. Do not include your account name or other personal information.

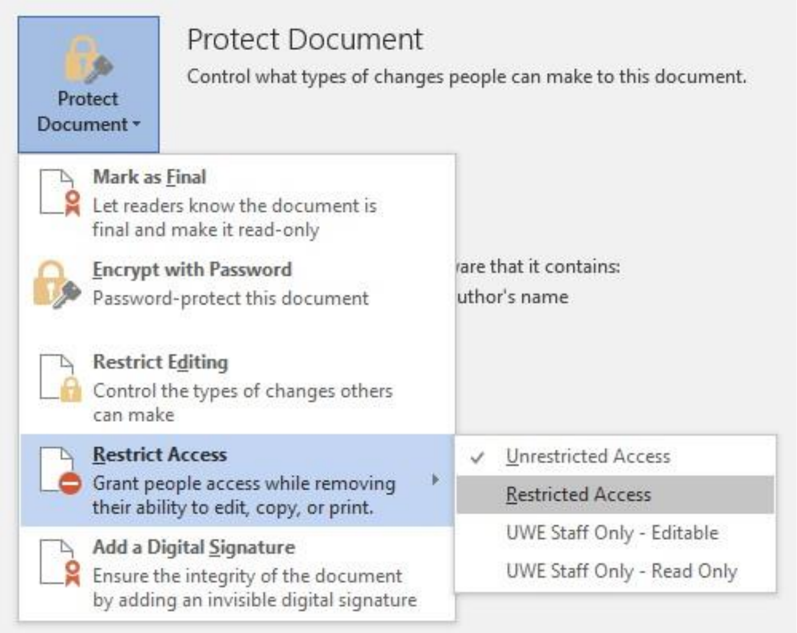
4. In the **Verify** box, type the password again, and then click **Set Password**.
5. Click **OK**, and then save your presentation.

Appendix G: Restrict Access to Microsoft files and document (Windows)

In addition to using 7-Zip and Microsoft password protection you could consider restricting access to Microsoft Office files.

For example, it is possible to specify the following:

- RESTRICTED ACCESS - Access for specific groups or people;
- UWE STAFF ONLY (EDITABLE) - Only UWE staff can view and edit a document;
- UWE STAFF ONLY (READ ONLY) - Only UWE staff can view a document.



Protect Document

Control what types of changes people can make to this document.

Mark as Final
Let readers know the document is final and make it read-only

Encrypt with Password
Password-protect this document

Restrict Editing
Control the types of changes others can make

Restrict Access
Grant people access while removing their ability to edit, copy, or print.

Add a Digital Signature
Ensure the integrity of the document by adding an invisible digital signature

Further information can be found at [UWE - Information Security Toolkit - Restrict Microsoft Office]

Appendix H: Device Encryption (Windows)

For UWE devices

All UWE laptops and desktop devices are encrypted using BitLocker encryption technology. Encryption is enabled as part of the standard build process and becomes 'active' as soon as a device is 'locked', or 'shut down.'

Mobile devices such as mobile phones and tablets are not encrypted by default. However, it is recommended that actions are taken to encrypt the device(s) when you take ownership.

For Non-UWE Devices:

Before you use any non-UWE managed devices (desktops, laptops and mobile phones) it is recommended that to access University data you should first ensure that you take precautionary measures to:

- Protect your personal devices with antivirus software;
- Turn on automatic software updates;
- Update your web browsers and any other relevant software.

You must not save confidential or restricted files to personal devices. Furthermore, you must not read, process or store confidential or restricted information on your personal devices.

Remember, that you should only be using UWE managed devices to read, process or store restricted or confidential information.

UWE acknowledges that as part of its working practices and processes its partners and third parties may require an understanding of encryption tools, in particular BitLocker and 7-Zip.

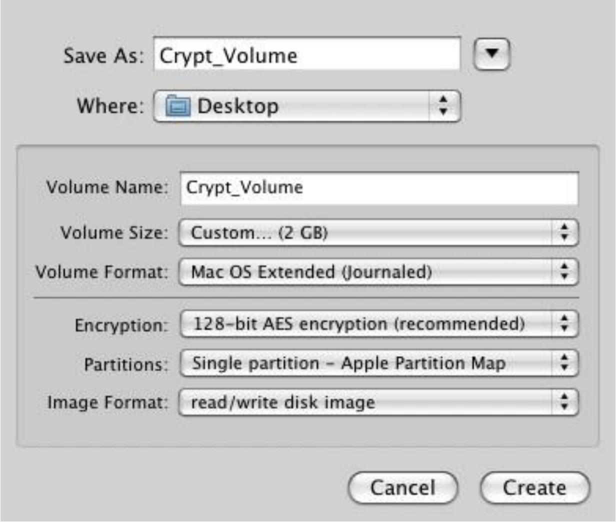
7-Zip is a free download for both personal use and commercial organisations. It can be downloaded from the main 7-Zip site: https://www.7-zip.org/download.html

Further guidance can be found at UWE - Information Security Toolkit - Encrypt Mobile Devices

Appendix I: Device Encryption (Mac)

The instructions below demonstrate how to create an encrypted disk image on a Mac, as a secure container for files. The steps here show the basic outline, but Apple change the details with each new version of the Operating System. Take these steps as a guide. A screenshot has also been provided:

1. Open Disk Utility found in the Utilities folder (/Applications/Utilities).
2. Click the New Image button, or choose New then Blank Disk Image from the Disk Utility File menu.
3. Enter a name in the Save As: field. This name is used for the disk image (.dmg) file.
4. Change the save destination if you wish to.
5. Change the volume name to match the disk image name.
6. Select a size for the image file from the Volume Size drop-down menu, or use Custom to set the space you require.
7. The default Mac OS X Extended (Journaled) volume format will be correct in most cases, if you wish to change it use the drop-down menu.
8. Choose an image format. You can use sparse disk image for a disk image that only uses as much space as it needs, rather than a set amount of space. If you're not sure use the read/write disk image choice.
9. From the Encryption: drop-down choose 256-bit AES if available, otherwise choose 128-bit AES to encrypt the image's contents with a password.
10. Click the Create button.
11. Enter and verify a good password in the dialog window that appears. This password will be saved in your keychain by default, it is recommended that you deselect this. Note: If you forget this password then the files stored within the disk image will be inaccessible. For guidance on strong passwords see UWE - Information Security Toolkit - Passwords
12. Click OK.



Save As: Crypt_Volume

Where: Desktop

Volume Name: Crypt_Volume

Volume Size: Custom… (2 GB)

Volume Format: Mac OS Extended (Journaled)

Encryption: 128-bit AES encryption (recommended)

Partitions: Single partition – Apple Partition Map

Image Format: read/write disk image

Data Protection Protocols

Appendix J: Further Information:

Visit an IT Service Desk or alternatively contact the desk by:

Telephone: 0117 32 83612; or Email: itonline@uwe.ac.uk

In addition, further information is available on the UWE - Information Security Toolkit pages