Principles for transferring personal data to and from collaborative partners

August 2017

University of Portsmouth
University House
Winston Churchill Avenue
Portsmouth PO1 2UP

T +44 (0)23 9284 8484

E: partnerships@port.ac.uk

W: port.ac.uk

Contents

Principles for transferring personal data to and from collaborative partners

Where we need to share personal data, sensitive personal data or confidential information with a collaborative partner (by email or any other data sharing technology), then the documents containing that data must always be transferred using the principles outlined in this document.

Applicability

These principles must be followed by all staff of the University of Portsmouth and all staff employed by any external partner organisation.

Scope

The principles described in this document apply to all personal data, sensitive personal data or confidential information transferred between the University of Portsmouth and an external partner organisation.

What is personal data?

Personal data identifies a living individual. For example, a name accompanied by other data about the individual such as address, age, telephone number, data regarding his/her financial status. Personal data can be an expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

What is sensitive personal data?

Personal data which identifies a living individual and includes any of the following types of data about that individual is considered to be sensitive personal data:

- Racial or ethnic origin;
- political opinions;
- religious beliefs;
- trade union membership;
- physical or mental health;
- sexual life;
- commission of offences or alleged offences

Source: Data Protection Policy (October 2013)

Principles of Transferring Personal Data

These principles refer to a secure system and strong passwords; you must make sure you apply to these principles.

1. The document containing the data to be sent (either to or from either the University or the collaborative partner) must be encrypted using at least 128bit AES encryption and using a strong password. The encryption used in Microsoft Office's Protect Document function (used to protect Word or Excel documents) is sufficient.
2. The password needed to encrypt/decrypt the document must be sent to a known and trusted contact at the destination using an 'out of band' method (i.e. a different method than email). Out of band could be:
   - landline telephone,
   - mobile phone,
   - Instant Messaging,
   - letter,
   - Skype chat or
   - by SMS text.

   Do not use a personal phone or a personal email account.
3. Once the document is encrypted, it can be attached to an email and sent to the collaborative partner or to the University, as the case may be.
4. Before you encrypt the data, always make a spare copy of the document you wish to send. If you encrypt your one and only copy and you forget the password, you will never get the data back.
5. The University and the collaborative partner are contractually responsible for adhering to data protection legislation and both parties must handle the data appropriately on a secure system.

Strong Passwords

A strong password must be at least ten characters long and should contain a mixture of capital and lowercase letters and at least one non-alphabetic character such as: >?!@*&% etc. Substituting letters for numbers can work well: e.g. Project>5tudent>3xam-2017

Password Changes

One strong password is required per complete data transaction (i.e. start to finish). The password is not reused for another transaction. A new password needs to be generated.

For example: UoP sends an encrypted form to Partner, Partner decrypts it, Partner adds the data to it and re-encrypts it and sends it back to UoP. UoP decrypts it using the same password. The next transaction will use a different password.

A Secure System Includes the Following Features:

- Access control – so only authorised staff have access to the data
- Encryption at rest – data is not stored as plain text or where it is not possible to have encryption at rest. The data must be stored in a secure data centre.
- No onward transfer of the data to another organisation
- Personal data and/or sensitive personal data must never be sent unencrypted under any circumstances

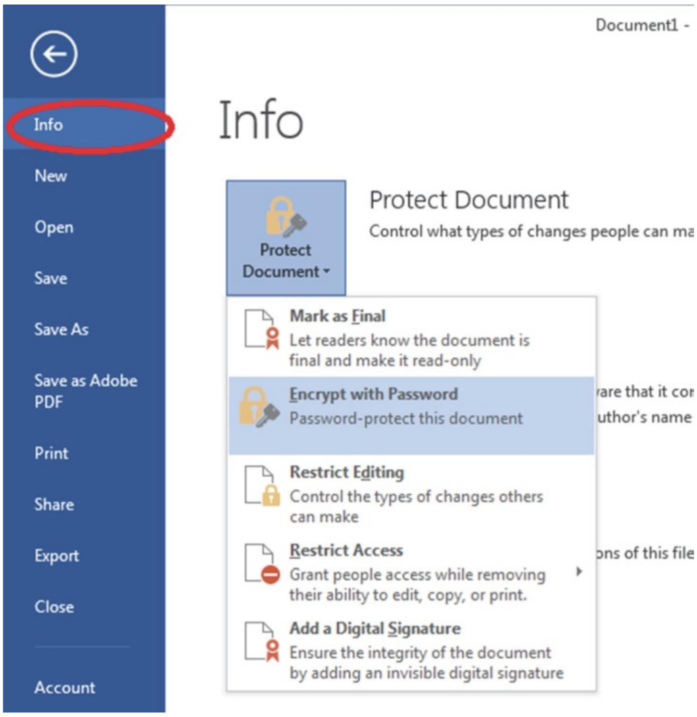
It is highly recommended that the above principles for transferring personal data are practiced first on 'dummy data' to ensure it is effective and to minimise the risk of data loss or compromise when live data is used.

Practicalities

Employing the principles for transferring personal data outlined above, there are three different software approaches outlined below. Please note, the specific 'how to' details may change over time as new software versions are installed. If in doubt, please seek advice from Information Services.

How to Use Microsoft Office Encryption

If the personal data is in a Word document or Excel spreadsheet, go to the 'File' menu in Word or Excel, then choose 'Info', the choose 'Protect Document', and then click 'Encrypt with Password'.



Control what types of changes people can ma

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

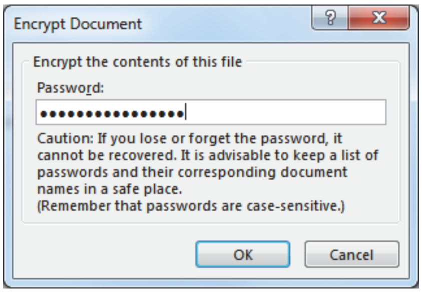
Encrypt with Password
Password-protect this document

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

In the ‘Encrypt Document’ pop-up box, enter a strong password (see guidance above) and click OK.



Encrypt Document

Encrypt the contents of this file

Password: ••••••••••••••••

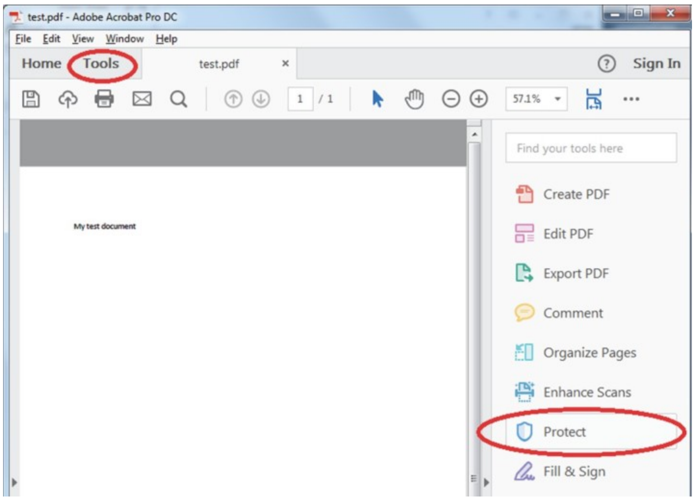
Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place.
(Remember that passwords are case-sensitive.)

A ‘Confirm Password’ box will pop-up to request that the password is entered again. When this is done, click OK. Save the document or spreadsheet as normal.

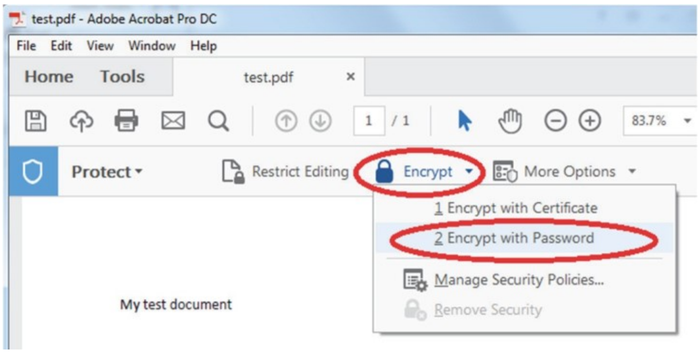
It is very important that you confirm that it has successfully been encrypted by opening the document again. If this is successful, it will require the password to open.

How to Use Encryption for Adobe Acrobat PDF

Open the PDF containing the personal data in Adobe Acrobat DC (not Acrobat Reader). In the ‘Tools’ section to the right of the document, choose ‘Protect’.



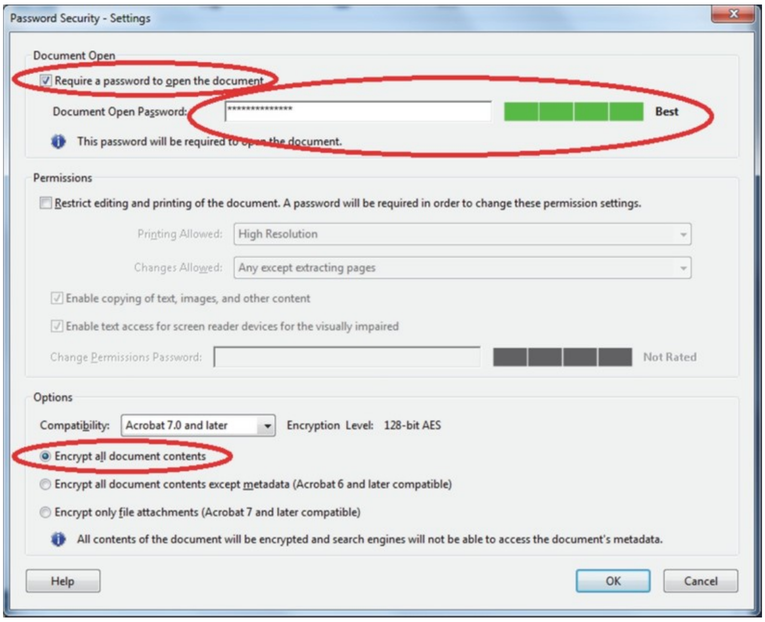
In the ‘Protect’ menu that appears above the document, choose ‘Encrypt’ and in the drop-down list, choose ‘Encrypt with Password’.



The ‘Password Security – Settings’ box appears. The ‘Option’ settings are set to ‘128-bit AES’ and ‘Encrypt all document contents by default, so there is no need to change them.

Tick ‘Require a password to open the document’ and type in the strong password into the ‘Document Open Password’ field. The bar chart to the right of the field indicates the strength of the password. Click ‘OK’

A ‘Confirm Document Open Password’ box will pop-up to request the password is typed in again. Click ‘OK’ and then save the document.



Password Security - Settings

Document Open

☑ Require a password to open the document

Document Open Password: ************** 🟩🟩🟩🟩 Best

This password will be required to open the document.

Permissions

□ Restrict editing and printing of the document. A password will be required in order to change these permission settings.

Printing Allowed: High Resolution

Changes Allowed: Any except extracting pages

☑ Enable copying of text, images, and other content

☑ Enable text access for screen reader devices for the visually impaired

Change Permissions Password: Not Rated

Options

Compatibility: Acrobat 7.0 and later Encryption Level: 128-bit AES

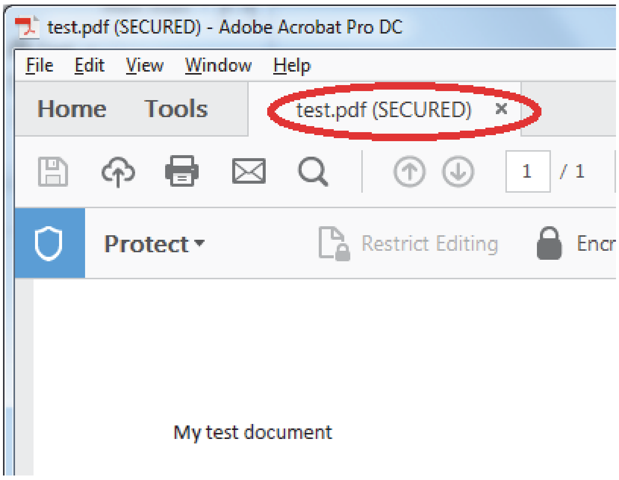
● Encrypt all document contents

○ Encrypt all document contents except metadata (Acrobat 6 and later compatible)

○ Encrypt only file attachments (Acrobat 7 and later compatible)

All contents of the document will be encrypted and search engines will not be able to access the document's metadata.

The document will now have the word ‘(SECURED)’ in the tab in Acrobat.



test.pdf (SECURED) - Adobe Acrobat Pro DC

My test document

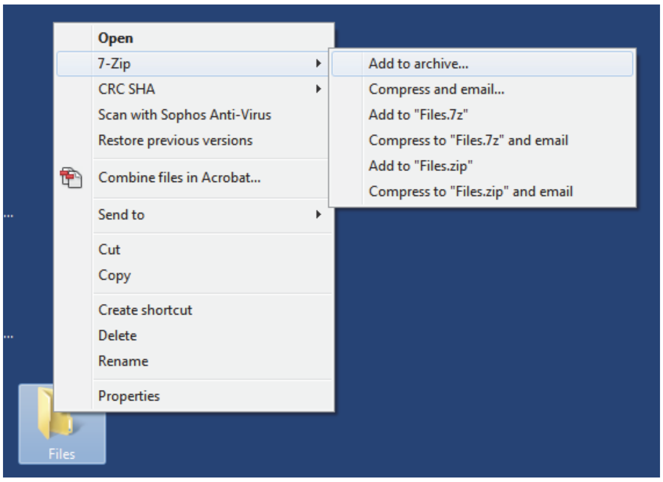
How to Encrypt Multiple Files

Depending on the technology used and the convenience, the following approaches can be used. For other approaches, please discuss them with the University’s Security Architect.

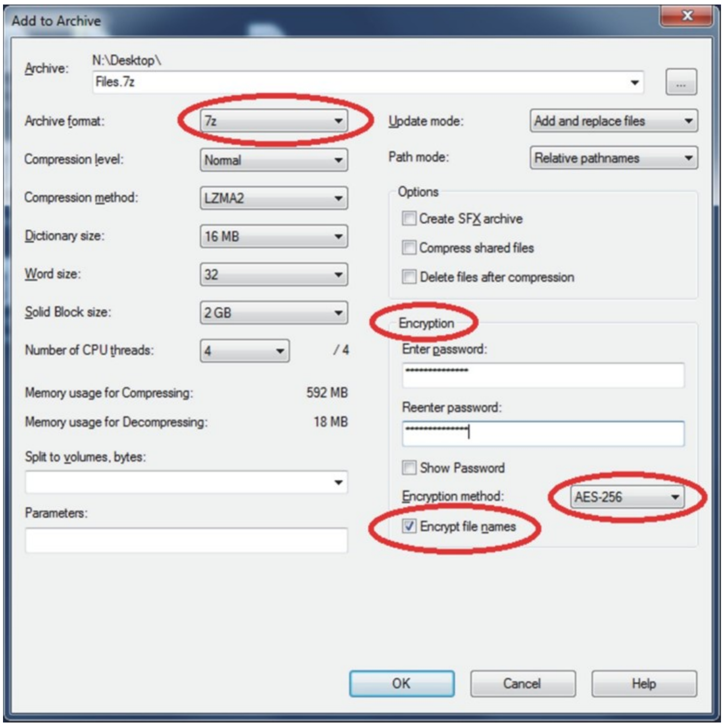
Using 7-Zip to make a ‘7-Zip (.7z)’ archive

Ensure 7zip is installed, either through AppsAnywhere or the 7-Zip website.

Right-click on the folder containing the files to be encrypted. In the menu, choose ‘7-Zip’ and in the pop-out menu, choose ‘Add to archive…’



In the ‘Add Archive’ box that appears, type a strong password in the Encryption section under ‘Enter Password’, and type the same strong password in the ‘Reenter password’ field. Ensure the ‘Encryption Method’ is set to AES-256 and ‘Encrypt File Names’ is ticked. Click ‘OK’.



Archive: N:\Desktop\ Files.7z

Archive format: 7z

Compression level: Normal

Compression method: LZMA2

Dictionary size: 16 MB

Word size: 32

Solid Block size: 2 GB

Number of CPU threads: 4 / 4

Memory usage for Compressing: 592 MB

Memory usage for Decompressing: 18 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: **************

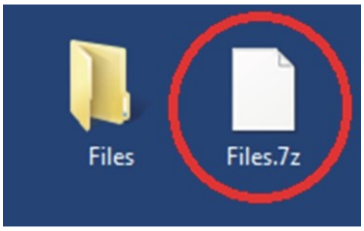
Reenter password: **************

☐ Show Password

Encryption method: AES-256

☑ Encrypt file names

The 7-Zip file produced will be encrypted and will appear in the same working directory that the original folder is in. Ensure you attach the 7-Zip file to the email.



7-Zip can also 'Zip' archive files. Ensure the 'Encryption Method' is set to AES-256 and the strong password is used. 7-Zip, or other Zip software capable of working with AES-256, must be used to decrypt the file.

Using Acrobat

Where it is not necessary to retain separate documents, these could be combined into one PDF, encrypted using a strong password and then emailed.

Use of Google Drive

Google Drive may be used. However, the documents uploaded to it must be encrypted and the password sent using an 'out-of-band' method, as described in the Principles for Transferring Personal Data section of this document. Care must be taken to ensure that the risk of documents being shared or forwarded to a third party is minimised.

If Your Email is Blocked

If a collaborative partner has security mechanisms that prevent University emails containing encrypted attachments from being received, both parties must work together to resolve the difficultly.

This may require the collaborative partner contacting their in-house IT department to find a solution to enable the emails are securely received. If a solution cannot be found, then the matter must be immediately escalated to the Head of Academic Standards, Quality and Partnerships.

Advice and Support

Should advice be needed on any aspect of information exchange, the University's Security Architect must be contacted.

Should advice be needed on whether something constitutes personal or sensitive personal data, the University's Data Protection Officer must be contacted. The University has wide experience in this area; if in doubt, ask.