


## SOP 06 INFORMATION SECURITY AND TRANSFERRING FILES

<b>VERSION NUMBER</b>	2.1	<b>DATE OF VERSION (dd/mm/yyyy)</b>	1	3	/	0	1	/	2	0	1	7
-----------------------	-----	-------------------------------------	---	---	---	---	---	---	---	---	---	---

<b>WRITTEN/REVIEWED BY</b>	<b>Print Name</b>	Jim Lumsden										
	<b>Position</b>	PhD student										
	<b>Signature</b>											
	<b>Date (dd/mm/yyyy)</b>	0	1	/	0	6	/	2	0	1	6	

<b>APPROVED BY</b>	<b>Print Name</b>	Alexander Board										
	<b>Position</b>	Research Associate										
	<b>Signature</b>	A.Board										
	<b>Date (dd/mm/yyyy)</b>	1	8	/	0	1	/	2	0	1	7	

<b>DATE OF NEXT SCHEDULED REVIEW (dd/mm/yyyy)</b>	1	3	/	0	2	/	2	0	2	1
---	---	---	---	---	---	---	---	---	---	---

<b>REVIEWED BY</b>	<b>Print Name</b>	Maddy Dyer										
	<b>Position</b>	Research Associate										
	<b>Signature</b>											
	<b>Date (dd/mm/yyyy)</b>	1	3		0	2		2	0	2	0	

Table of Contents	Page
1. PURPOSE	2
2. PERSONNEL REQUIRED AND LEVEL OF EXPERTISE	2
3. MATERIALS AND EQUIPMENT REQUIRED	2
4. USEFUL READING	2
5. PROCEDURES	2
5.1. What constitutes confidential information?	2
5.2. Sharing confidential files within TARG	3
5.3. Sending confidential files to a non-TARG member	8
6. TROUBLE SHOOTING	10

Definitions/Abbreviations	
SOP	Standard Operating Procedure
TARG	Tobacco and Alcohol Research Group
UoB	University of Bristol

## SOP 06

# INFORMATION SECURITY AND TRANSFERRING FILES

---

### 1. PURPOSE:

- To provide step-by-step instructions to all persons needing to store and transfer confidential information on and between computers.

### 2. PERSONNEL REQUIRED AND LEVEL OF EXPERTISE:

- Investigator or research team
- Must complete the University Data Security Training  
[https://www.bris.ac.uk/is/media/training/uobonly/datasecurity/page\\_01.htm](https://www.bris.ac.uk/is/media/training/uobonly/datasecurity/page_01.htm)

### 3. MATERIALS AND EQUIPMENT REQUIRED:

- If on Windows:
  - 7-zip ( <http://www.7-zip.org/> ) (should be installed by default on all university computers)
- If on Mac:
  - Keka ( <http://www.kekaosx.com/en/> )

### 4. USEFUL READING:

- The main University site on data security, containing comprehensive guidelines to storing, handling and destroying confidential data: <http://www.bris.ac.uk/infosec/uobdata/>  
Short and useful sublinks (well worth reading):
  - Working offsite: <http://www.bris.ac.uk/infosec/uobdata/offsite/>
  - Encryption flowchart: <http://www.bris.ac.uk/infosec/uobdata/encrypt/>
  - Think Twice guidelines: <http://www.bris.ac.uk/infosec/uobdata/thinktwice/>
  - Using mobile phones, tablets and laptops: <http://www.bris.ac.uk/infosec/uobdata/mobile/>

### 5. PROCEDURES:

#### 5.1 *What constitutes confidential information?*

Confidential information, otherwise known as 'personal data', means information that relates to an identifiable living individual, and which may permit an individual's identification. This includes obvious personal data such as names and addresses, but also combinations of data that may leave a subject identifiable. For example, if it is known that the participants from a study were drawn from the university, then a combination of gender, age and subject could be sufficient to identify the individual. Additionally, personal information may include any expression of opinion about a person, and even meta-data about handling that person's information. Additionally, although it may sometimes seem farfetched that an individual might be identified from the data you have collected, the Data Protection Act stipulates that data should be secure against very rigorous investigation.

For more information see:

<https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf>

#### 5.2 *Sharing confidential files within TARG*

If you need to share files containing confidential information with another member of TARG for a long period of time, in order to collaborate on data analysis or entry, then the best way to do this is via the shared Z-drive.

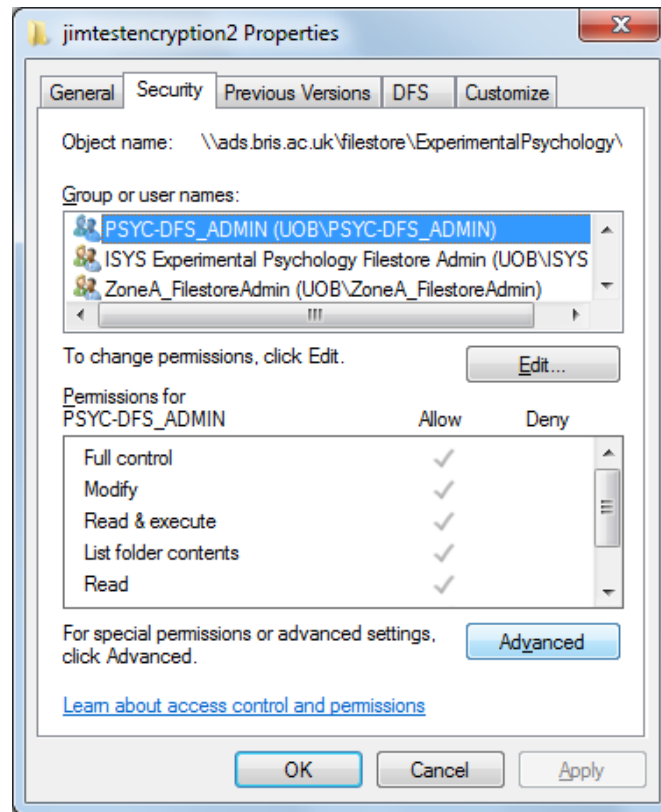
---

## SOP 06

# INFORMATION SECURITY AND TRANSFERRING FILES

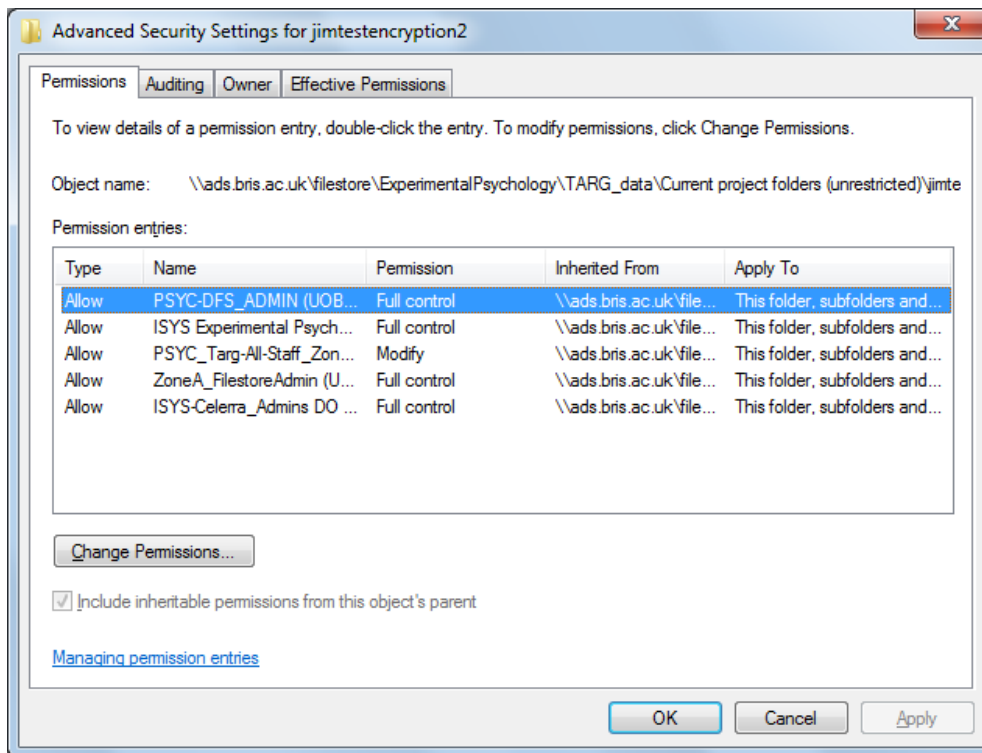
---

Go to [\\ads.bris.ac.uk/filestore/ExperimentalPsychology/TARG\\_data/Current\\_project\\_folders\\_\(unrestricted\)](\\ads.bris.ac.uk/filestore/ExperimentalPsychology/TARG_data/Current_project_folders_(unrestricted)) . Create a new folder, giving it an appropriate name. Then right click that folder, and choose “properties”. As shown in the screenshot below, navigate to the security tab and click the button at the bottom labelled “Advanced”.

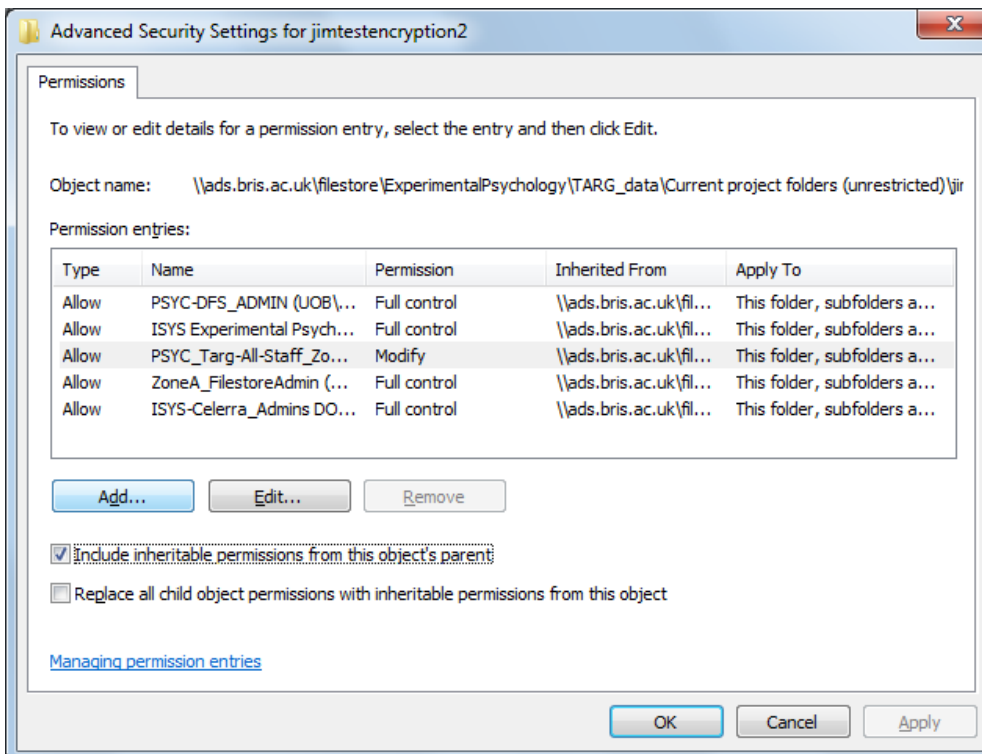


This takes you to the advanced security settings panel. As shown in the screenshot below:

## SOP 06 INFORMATION SECURITY AND TRANSFERRING FILES



Next, click the “Change Permissions” button which will move you to a very similar screen, except on this screen the bottom checkbox “Include inheritable permissions from this object’s parent” will be toggle-able.

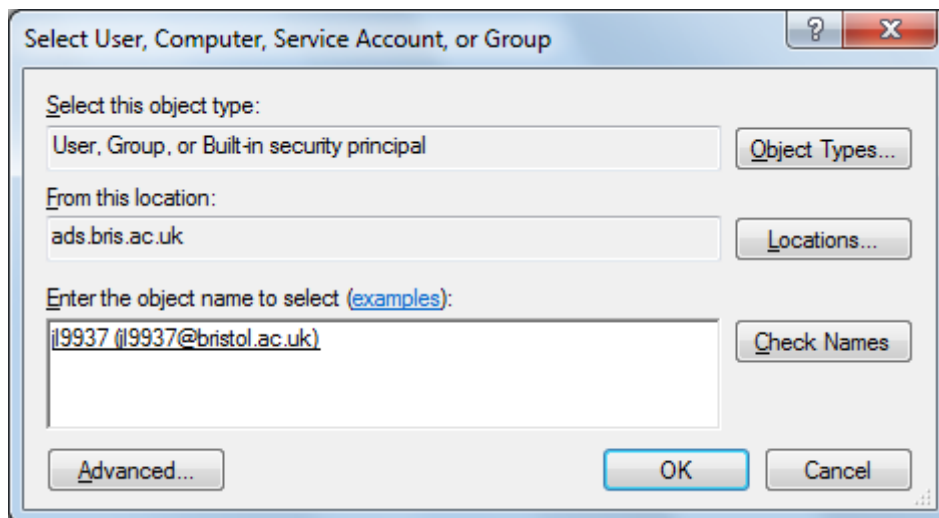


## SOP 06 INFORMATION SECURITY AND TRANSFERRING FILES

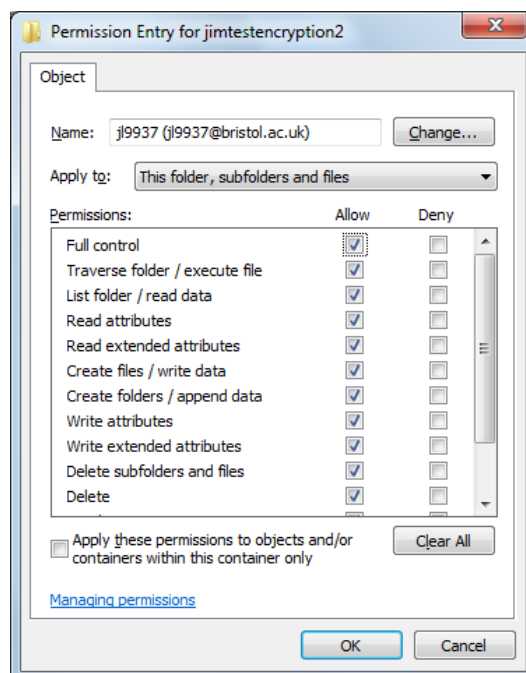
Click the “add” button to open up a new box which allows you to add security access to your new folder, this is shown in the next screenshot. In the text-box entitled “Enter the object name to select” you can type the username of a student/staff member who you want to have access to this folder. If you type “j19937” and then click the “Check Names” button, the system will search for j19937 and add his full user object. If the system recognises the user then they will be underlined.

Notes:

- Usernames are often the same as email addresses.
- When setting up a secure folder for a project, be sure to add yourself first. If you do not include yourself then you will lose access to the folder after you change these security settings.

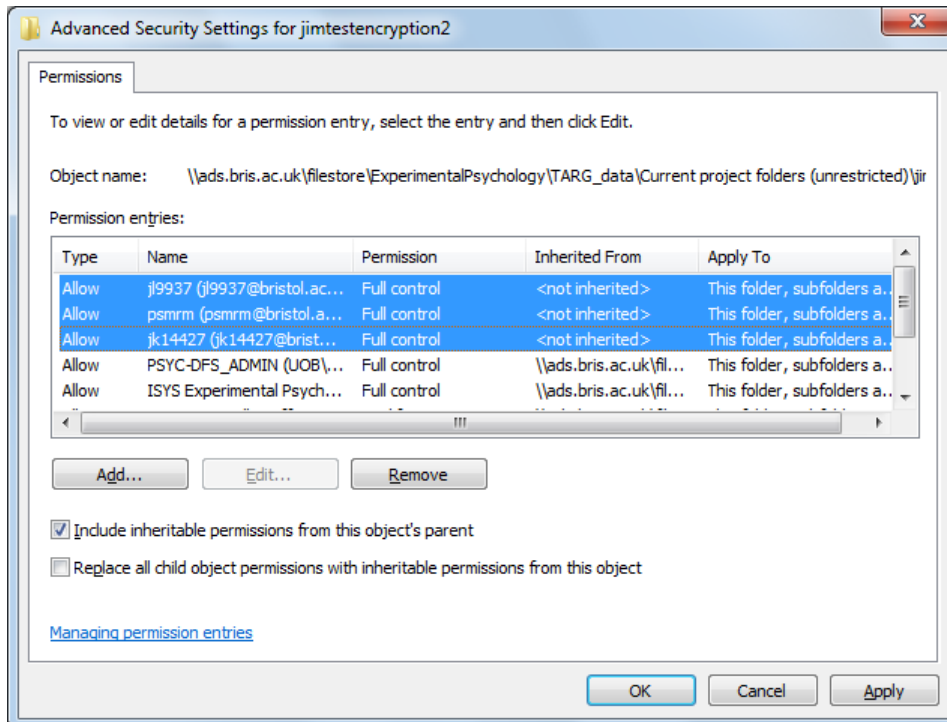


Click “OK” and you will be taken to another security screen where you can assign powers to the user you just entered. Tick the “Full Control” checkbox, as shown below, and then “OK”:

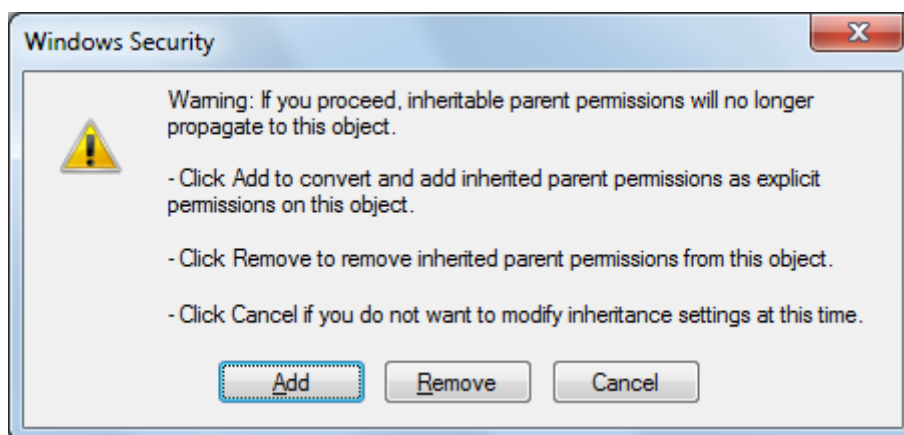


## SOP 06 INFORMATION SECURITY AND TRANSFERRING FILES

Once you have added one user (which ought to be yourself) you may repeat the above step until all required users are added. When you are done, the security settings window may look like this (in this case, Jim Lumsden, Marcus Munafò and Jasmine Khouja have been given access rights) :



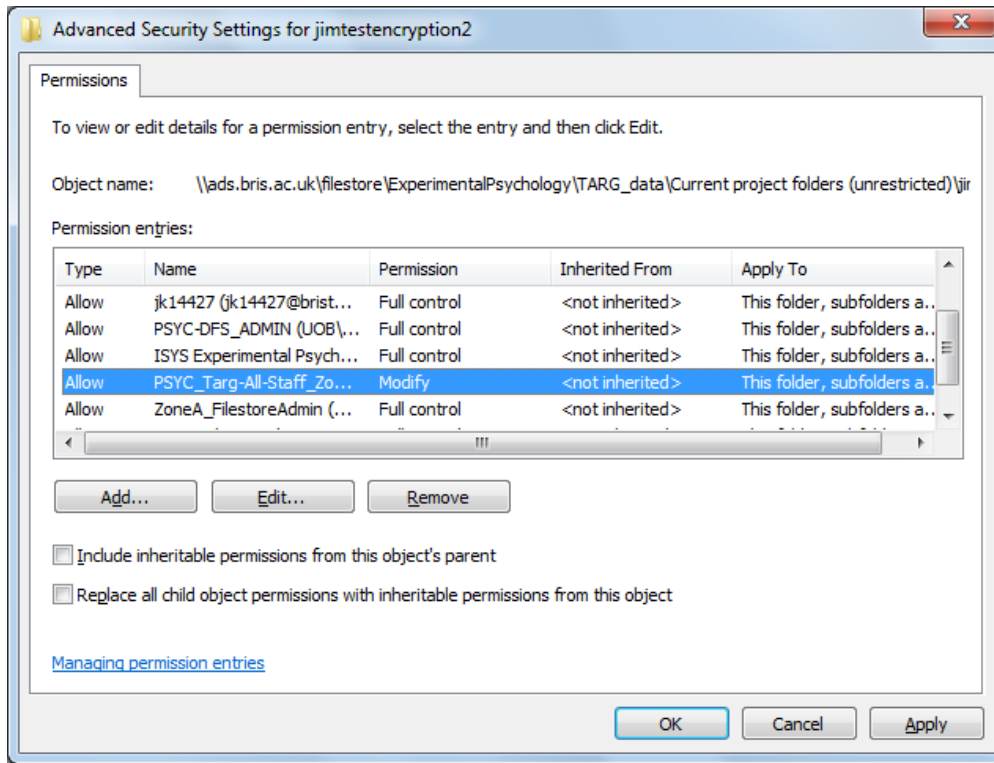
Having added these users as separate objects, we must now deny access to this folder to any other members of TARG who ought not to see the data. Firstly, uncheck the checkbox "Include inheritable permissions from this object's parent". When you do so, a window will pop-up stating:



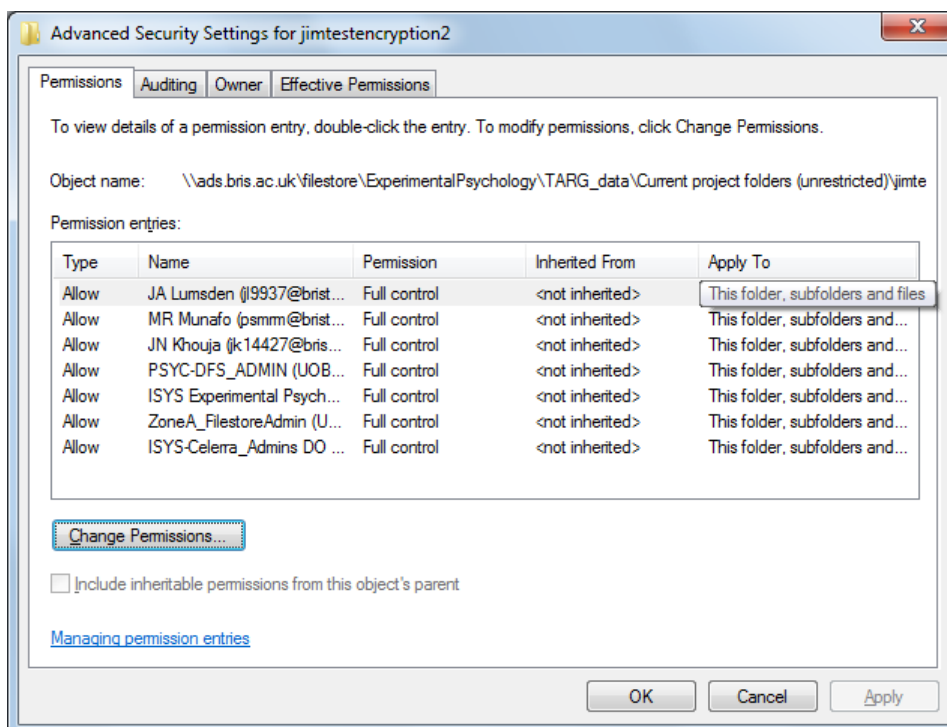
Be sure to click the "Add" option.

Back in the advanced security settings window, scroll down the list of permissions until you find PSYC\_Targ-All-Staff\_Zo.... Highlight it and press "Remove".

## SOP 06 INFORMATION SECURITY AND TRANSFERRING FILES



You can now press OK and return to the main security screen where all your final settings will be displayed. It should look something like the screenshot below, with the new users at the top. Press "OK" and "OK" again to return to the TARG Z Drive.



---

## SOP 06

# INFORMATION SECURITY AND TRANSFERRING FILES

---

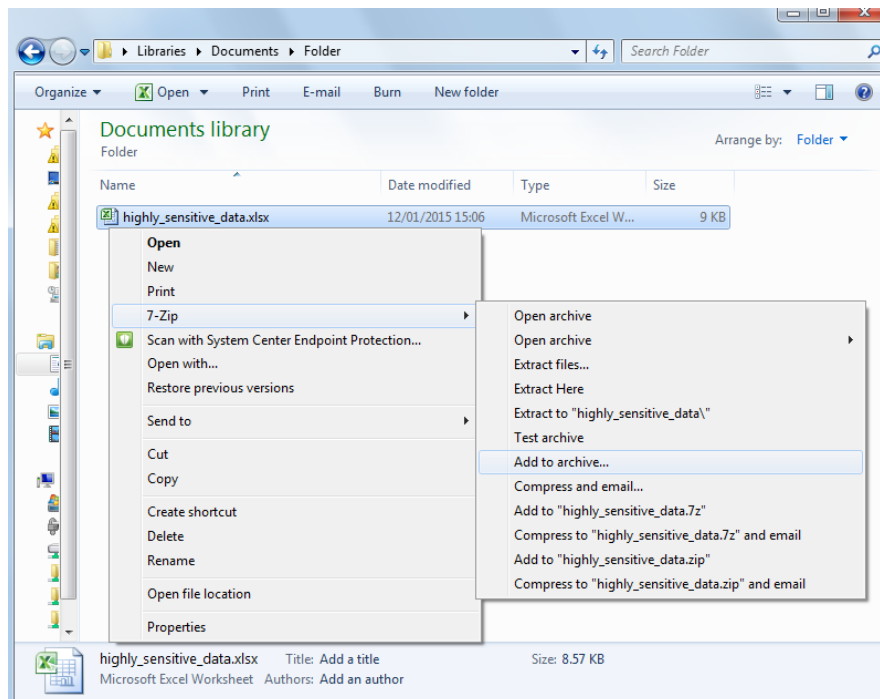
The folder you have now created is secure and cannot be accessed by anyone other than those users you added above. You can use this folder to store confidential files, and share them with other users who you added.

### 5.3 Sending confidential files to a non-TARG member

You must not send files containing personal information in an unencrypted format. If a file is encrypted and it is small enough in size that it can be attached to an email and sent, then that is ok. Otherwise you will need to use the university file sharing service “Fluff”.

**Warning:** you must never use Google Docs or Dropbox to store/share confidential information as we cannot guarantee that either of these cloud-storage services provides strong enough encryption to meet the requirements of the data protection act.

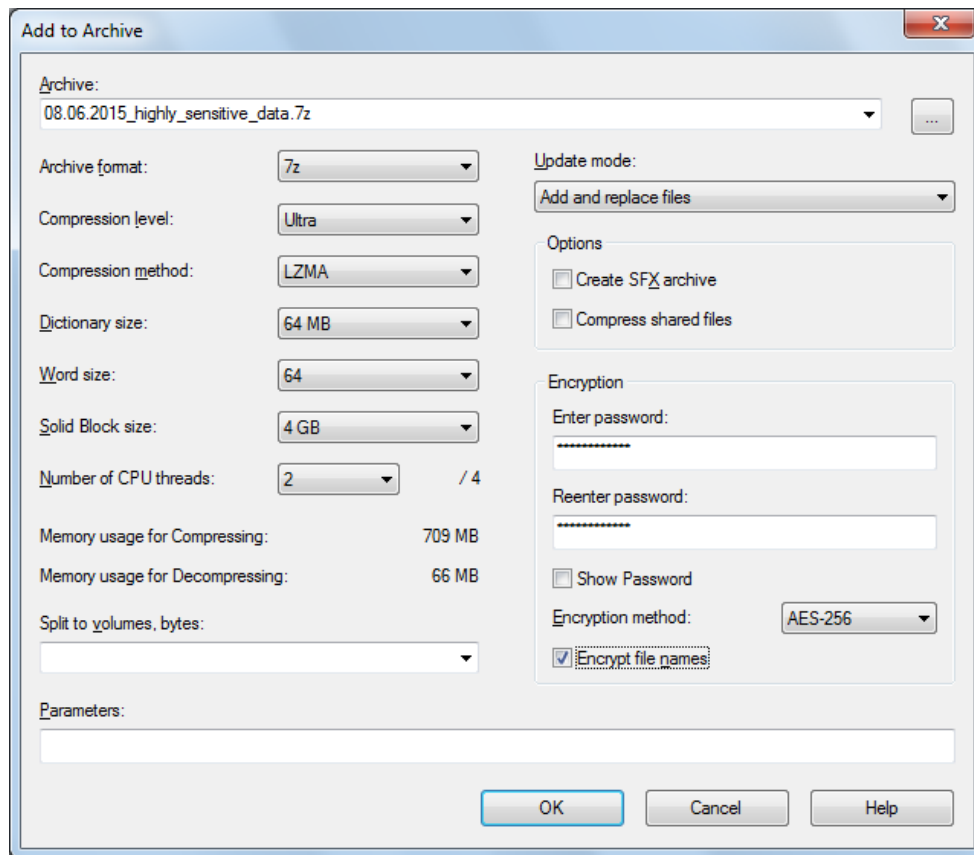
Firstly, right click the file you wish to encrypt: select “7-Zip” and “Add to archive...”



This will open a new window with the following options. Set all the options as shown below, and enter a strong password.



## SOP 06 INFORMATION SECURITY AND TRANSFERRING FILES



When you press ok, a new .7z archive will be created. Double clicking on it should open a new window which requires a password in order to proceed. At this point, your file is secure; all that remains is to send it.

If the .7z file is smaller than 5mb you may send it via the university email system. Simply attach the .7z file to an email, send it, and then call the recipient and deliver the password over the phone. Remind the recipient to avoid writing the password down on a post-it note and sticking it to their computer. All the encryption in the world cannot stop someone who acquires the password from a carelessly placed note.

If the .7z is larger than 5mb, or you need to share it with multiple people, then Fluff is the best option (<http://fluff.bris.ac.uk/fluff/>). Upload your .7z file, and then email the fluff link to your collaborators. Again, once the encrypted file is sent you must call the recipients and tell them the password.

**N.B.** Do not send the password to the encrypted file by email.

### 6. TROUBLE SHOOTING:

Problem	Solution
Advice and guidance:	<p><b>Data Protection Departmental Representative (Psychology)</b>  <b>Melissa Werrett</b>                      (0117) 954 6998 internal 46998  <a href="mailto:Melissa.Werrett@bristol.ac.uk">Melissa.Werrett@bristol.ac.uk</a></p> <p><b>UoB Information Security Team</b>  <a href="mailto:infosec-feedback@bristol.ac.uk">infosec-feedback@bristol.ac.uk</a></p>

---

**SOP 06**  
**INFORMATION SECURITY AND TRANSFERRING FILES**

---

Technical support:	<b>IT service desk</b> <a href="mailto:service-desk@bristol.ac.uk">service-desk@bristol.ac.uk</a> (0117) 928 7870 internal 87870
Any other problems:	<b>TARG Laboratory phone:</b> 07957334265  <b>Marcus Munafò</b> (0117) 954 6841 internal 46841 <a href="mailto:Marcus.Munafò@bristol.ac.uk">Marcus.Munafò@bristol.ac.uk</a>