

Working Instruction (WI) Summary Box

|  |  |
| --- | --- |
| WI Title | Sending of encrypted data via email (Non-Identifiable Data Only) |
| WI Index Number | WI15 |
| Version | V2.0 |
| Version Date | 08 December 2022 |
| Lead Author | Tracy Whitehurst |

|  |
| --- |
| DISCLAIMER  This WI is the property of the Keele School of Medicine (SOM) and Keele Clinical Trials Unit (Keele CTU), Keele University and the content cannot be reproduced without specific permission from the owner.  Any superseded versions of this document need to be promptly withdrawn from use.  Updates to this document will be via the Author. All individuals undertaking functions outlined in this document are responsible for ensuring that they are trained in the procedures outlined in the correct version of this document. |

**Version History Log**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date Approved | Reason(s) for Change | Implementation Plan |
| 1.0 | 06-Dec-2019 | New Working Instruction |  |
| 2.0 | 08-Dec-2022 | Updates relating to new School of Medicine, retirement of sendfile system and implementation of Microsoft OneDrive |  |

**Table of Contents**

[1. Purpose 3](#_Toc103614914)

[2. Procedures 3](#_Toc103614915)

[2.1 Verify Data Receiver 3](#_Toc103614916)

[2.2 Data Encryption Process 3](#_Toc103614917)

[2.3 Data Transfer Process 4](#_Toc103614918)

[2.4 Removing a file 6](#_Toc103614919)

[3. Key Personnel to whom this SOP Applies 7](#_Toc103614920)

[4. References 7](#_Toc103614921)

# Purpose

Providing instructions of sending encrypted data via Microsoft OneDrive and Microsoft Teams, this should only be used for Non-Identifiable Data. Release of Participant Identifiable data is not permitted unless in extreme circumstances and with approval following Governance regulation conditions.

It is advisable for another appropriate member of centre staff to review the data file before transmission to confirm no patient identifiable data is contained in the data file/s.

If research data set are requested for release it is the responsibility of the CI to ensure correct permission is in place from the sponsor and funder to allow subsequent release of study data and the permission provides the legal basis for data reuse.

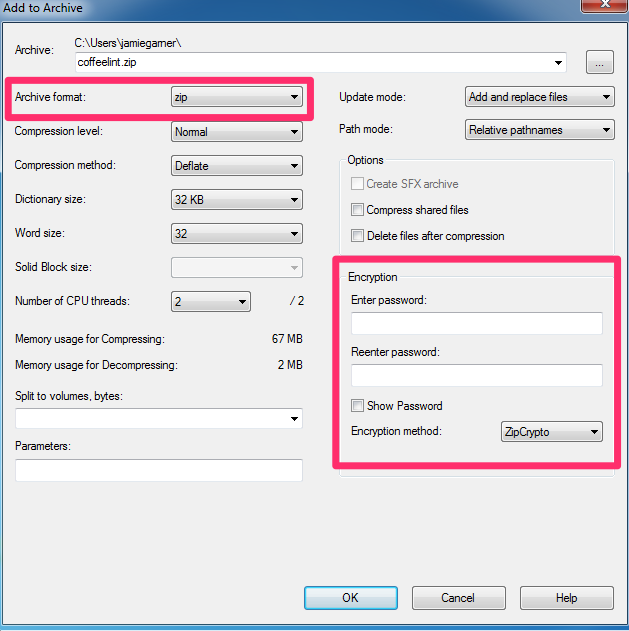
# Procedures

## Verify Data Receiver

Prior to data transfer assurances must be confirmed to verify that the person receiving the data is the accurate and intended recipient for the data.

1. Obtain the name, email address and contact telephone number of the intended data receiver.
2. Send an email from your account with the following format to the data receiver:
   1. Subject: Confirmation of receiver email address
   2. Email content: Please reply to this email with your direct dial number confirming that you are the intended recipient of this email.
3. Call the data receiver and confirm that the email has arrived. If they have not received the email repeat the step 1 and 2, until confirmation has been received back via email.

## Data Encryption Process

1. Upon email confirmation create a password protected zip file:
2. In Explorer highlight the file/s for transfer
3. Right click on it/them and select 7-Zip
4. Click on “add to archive”
5. Give the .zip archive file an appropriate name, consider the file storage location
6. Set the archive format to zip
7. Set a password in the Encryption section. *The password should be at least 8 characters long and include at least one capital letter, one lower case letter, one special character (for example (!@£$%^&\*()-=+\_][{}) and one number.*
8. Set the Encryption method to ZipCrypto
9. On completion click [OK], the archive file will be created and saved in the file location you specified.  **

## Data Transfer Process

To make the .zip archive file available to the intended recipient there are two options detailed below:

Personal One Drive

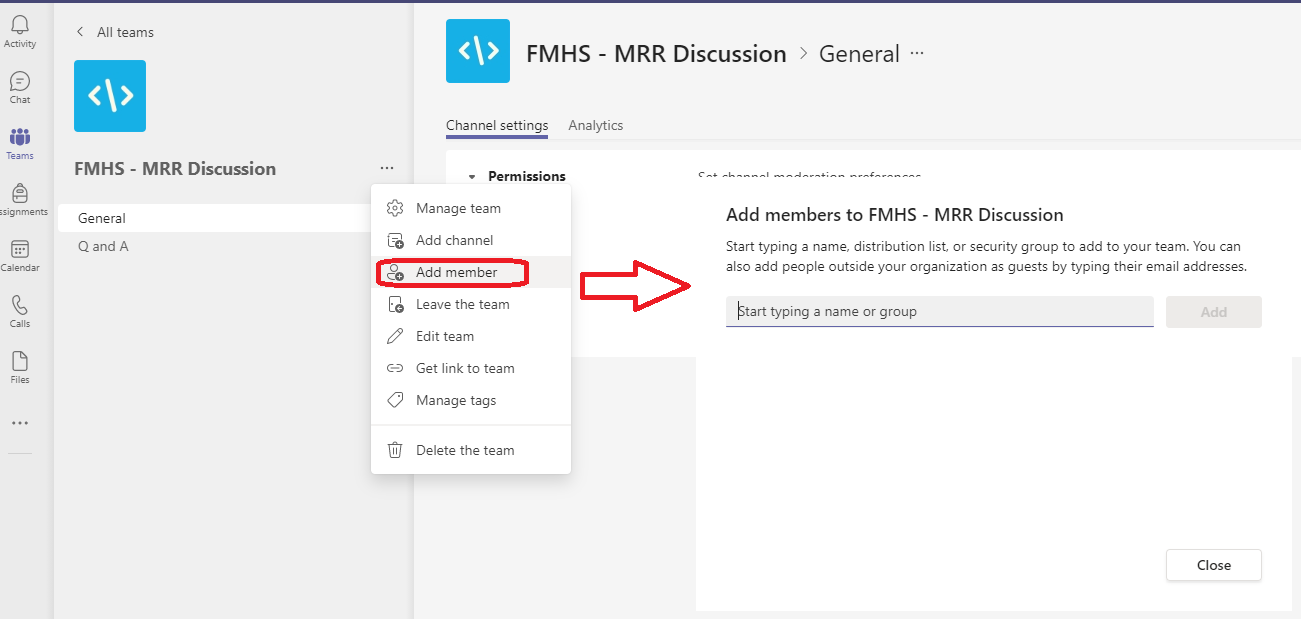
It is recommended to use this method for files which are to be shared on a one-off basis or where minimal sharing is needed.



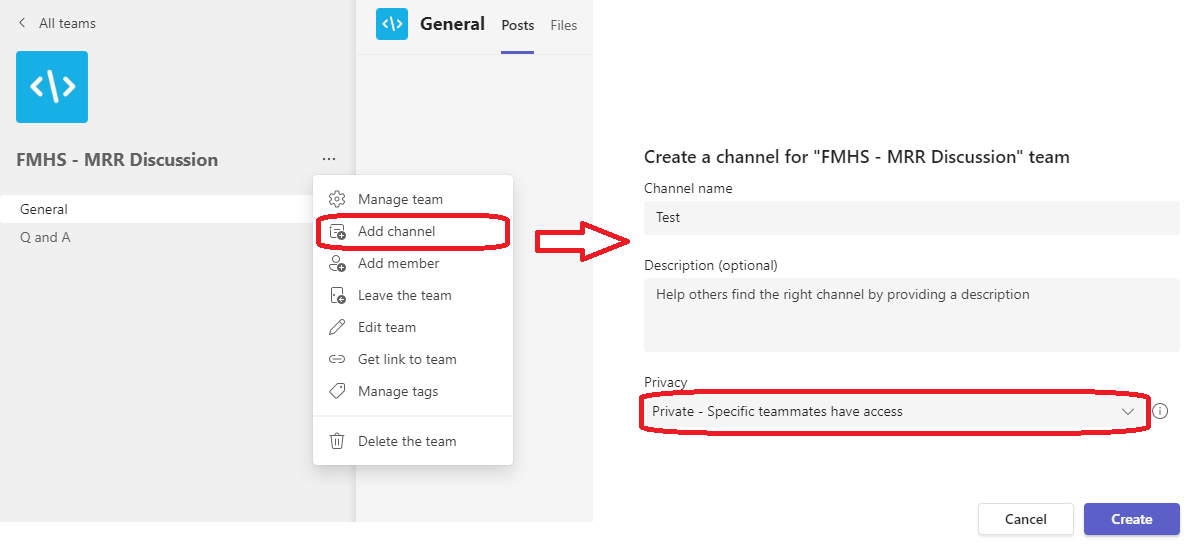
Once the folder has been created in your OneDrive folder, right click on the folder, click on share and the pop-up shown in the image will appear. You can either send the link directly by adding the email address to the ‘To’ box and adding a message. Or you can copy the link using the icon in the bottom left corner and include the copied link into an email to the recipient. To ensure that the recipient can edit the data change the drop-down icon highlighted green to ‘Can edit’.

Microsoft Teams – Restricted channel accessible only to the data custodian and requester

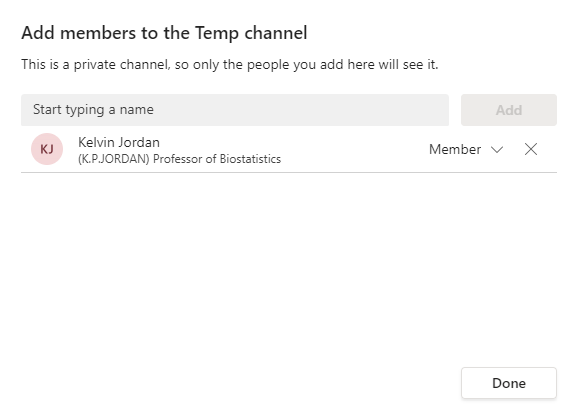
This method should be used when recurring shares with the team will be necessary (for example when the data recipient is a project team member).

In the project specific Microsoft Team, next to the Team name in the left navigation bar, select the 3 dots (…) and then select the add member option. In the pop-up box you will then be asked to enter the recipient’s email address. Please ensure the correct email is entered. Once entered click on the “Add” button. The recipient will then have access to the team.

The data should be held within a private channel. The recipient will have to be added to the channel before they will have access to the data. To create a private channel click on the 3 dots (…) next to the Team name, Click on “Add channel”, In the pop up box add the name of the channel in the “Channel name” box. Make sure to change the “Privacy” drop down box from “Standard – everyone on the team has access” to the “Private – Specific Team members have access”. Click on the “Create” button.

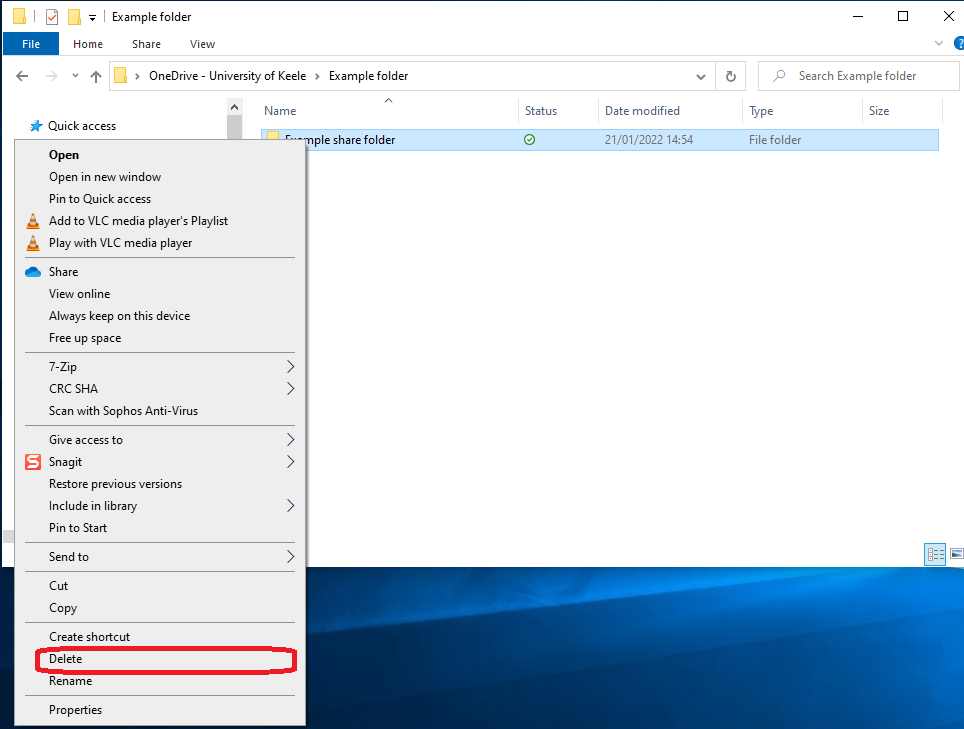


Another pop-up box will appear, in the input box add the names of the data recipient and data custodians and click on the “Add” button. Once you have added all the members to the channel required, click on the “Done” button. Only these people, and the person who created the channel, will now have access to the channel.



## Removing a file

To remove a file follow the steps below set out for each of the 2 data transfer methods.



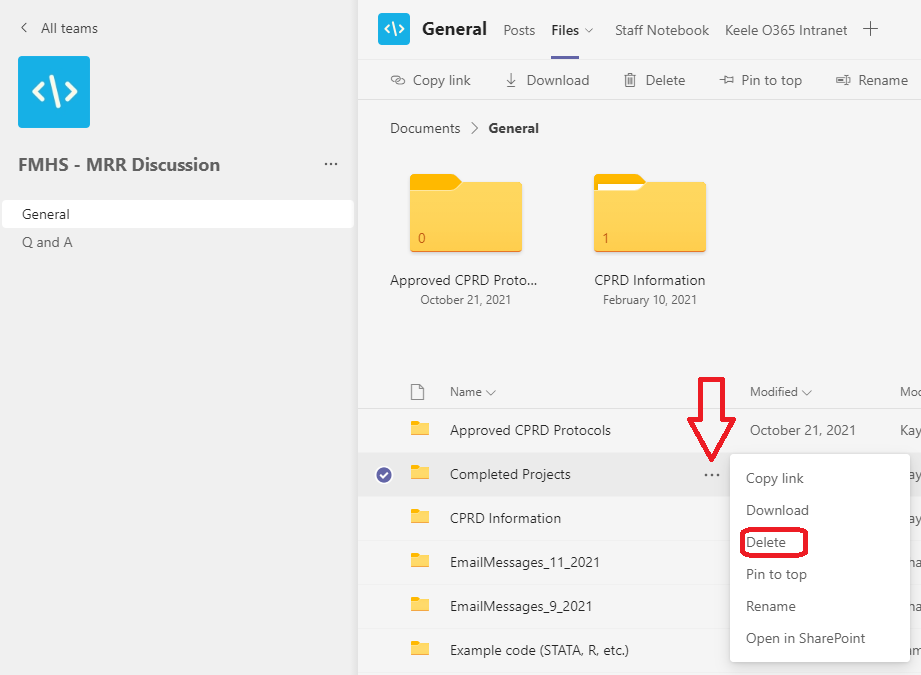
Personal One Drive

The shared folder containing the data should be deleted. Right click on the folder which has been shared with the recipient and select the delete option from the drop-down menu. This is highlighted in the image to the right.

Microsoft Teams

The data files shared with the recipient should be deleted from the ‘files’ section of the Microsoft Team private channel.

To do this locate the folder containing the shared data. Click on the three dots to the right of the folder name and select the delete option as highlighted below.



# Key Personnel to whom this SOP Applies

Any person sending non identifiable data to an approved data recipient.

# References

None