Doing good together

File Sharing Policy

Doing good together

Document Control

Proprietary Information

The content of this document is considered proprietary information and should not be disclosed outside of the The Midcounties Co-operative (TMC).

Document Version Control	
Title	File Sharing Policy
Data Classification	Internal
Document Owner	Sheridan Hindle
Document Author(s)	Sheridan Hindle
Document Approver(s)	Sheridan Hindle/Sean McGovern
Review Period	12 Months
Last review date	
Next review date	

Document History			
Date	**Version**	**Version reason**	**Author**
20/08/2024	0.1	Draft	Sheridan Hindle
30/08/2024	0.2	Updated edits	Sheridan Hindle
18/10/2024	1.0	Final	Sheridan Hindle

Doing good together

Contents

Doing good together

1. Scope

Sharing of any file internally and externally with colleagues or third parties. This includes files held locally on laptop/desktops, file servers and Microsoft 365 including OneDrive, SharePoint, Teams or any other Microsoft application.

2. Responsibilities

The Information Security Manager is responsible for ensuring that all file sharing takes information security into account in the first instance.

All Data Protection Champions are responsible for ensuring that colleagues in their teams are aware of their file sharing responsibilities.

3. File Types

This policy is applicable to all file types including but not limited to documents, spreadsheets, read only files and digital streaming files such as mp3 and mp4. Emails that are attached to other emails are included as these are a file type of their own and could contain other files.

4. Background

Every day many files are shared internally and externally with other colleagues and third parties using various means. Many are sent via email as attachments. Any file that is shared can potentially be shared further by the recipient. Where these are third parties you cannot always be sure they apply the same controls as Midcounties. Care must be taken to ensure it is safe and appropriate to share data and the most appropriate means of sharing must be used.

5. Storing Files

Several options are available to store files. These include file servers, SharePoint, OneDrive and Teams.

Files should never be stored locally on a desktop/laptop or smartphone. All these devices fail over time, can be lost or stolen or become corrupt. They are not backed up either, so any data is lost when they fail.

Files should not be stored or shared on portable storage devices such as USB Sticks. These are easy to steal, can often contain malware and are disabled by default for use with company laptops and desktops.

The recommended approach is to use SharePoint, OneDrive or Teams. All these have group sharing functionality as well as the capability to share individual files and folders permanently or on a temporary basis as read only or editable files.

File servers are an acceptable place to store files but are not as easily shared with third parties or colleagues not within your team.

Doing good together

6. Should the File be Shared?

The questions you should ask yourself before sharing data with someone else include:

- Does the recipient require all the data in the document. Where possible, the amount of data should be reduced to what is essential to be shared.
- Does the person already have access to it. If the person you are sharing a file with is a colleague, they may already be able to access it so you may only need to signpost them to the file.
- Does the person need permanent access to the data. If you send the person a file attachment via email they will have the data permanently. If you share a link that is time limited, then they have access only when they need it which is more secure.
- How sensitive is the data in the file. If the data contains information about people or confidential company information you will want to choose the most secure way of sharing the file with the recipient whether internal or external.
- Do you share the data regularly with the same colleague or third party. If so, it may be better to automate file sharing using a secure transport mechanism rather than manually sharing files.
- If it is a third party, do we have a non-disclosure agreement (NDA) or contract in place to support sharing of files. Also, is there an approved data security questionnaire (DSQ) in place.

7. Secure Ways to Share Data

If after reviewing the information in this document, you decide the file needs to be shared the best way to share the file needs to be chosen.

a. Internally with Colleagues

The most secure way to share files with colleagues internally is to either give them access to the location of the file if they need regular access or to send them a link.

If a link is going to be sent, then the following options should be used when creating the link:

- Share it with only the people you choose.
- Ensure sharing is set to 'Can view' unless you want the person to edit the file.
- Set an expiration date for sharing and the expiration date should be as short as possible.

The link can be emailed or sent via Teams to enable the colleague to see the file in question.

b. Externally with Third Parties

Many third-party organisations are used to handling sensitive data and may have their own solutions for doing so, for example their own secure file transfer site or Mimecast. If the third party is in contract, has an NDA and has a DSQ which includes the solution being in used this will be the best way to share data.

If the third party does not have a solution there are several other ways data can be shared including a link as described in (a). The options including their strengths and weaknesses are outlined below:

- Secure File Transfer (SFTP)
  Required a username and password to access the file. Good for sending large volumes of files to a third party or receiving from them. Easy to automate. Remember a strong unique password should be used of at least ten characters and contain letters, numbers, special characters and have some lower-case and upper-case characters as per policy.
- Using a SharePoint Site
  Easy to setup. Do not share links externally. Raise a request with the IT Helpdesk to have a secure shared area created in SharePoint.
- As an Email Attachment
  This is the option of last resort as the least controllable and least secure. One a file is attached to an email you have no control over where it goes next, who sees it or for how long. If a file must be sent by email it should be password protected. You should be cautious of placing too much reliance on passwords as there are free tools and readily accessible tutorials on how to get round passwords on documents.

c. What if None of the Options are Appropriate?

If the options listed above are not suitable, contact IT through ServiceNow.

Doing good together

Sharing Data Key Guidance

Key Contact

Information Security and Risk Manager – Sheridan Hindle
Society Data Protection inbox - Data-Protection@midcounties.coop
Society's Data Protection Officer – Sean McGovern, Head of Legal Services

Summary

Files are often shared with colleagues and third parties. These files can include sensitive data and need to be protected. Listed below are the recommended actions for storing and sharing files with colleagues and third parties.

Storing Files

Use the following as a guide for storing files safely and securely:

- Never store files on your Laptop/Desktop/Smartphone, these are not backed up.
- Never store files on portable storage such as USB sticks. These can contain malware and are easily lost.
- Storing files on a file server is secure and good for shared access with the colleagues in your team.
- Storing files on Teams/SharePoint/OneDrive allows you to easily share links to files via teams and only give the right people, the right level of access, for the time they need it.

Sharing Files

Use the following as a guide for sharing files:

- Does the recipient require all the data in the document. Where possible, the amount of data should be reduced to what is essential to be shared.
- Use email as a last resort as it is the least secure. If you must use email, then password protect the file if it contains sensitive information. You should be cautious of placing too much reliance on passwords as they are easily bypassed with free and readily available tools.
- If sharing with colleagues internally use a link within Teams/SharePoint/OneDrive for ad hoc sharing. Make sure you share with individuals not with everyone and limit the time they have access to it. Only give someone edit access to a file if necessary. If the colleague needs permanent access add them to the folder rather than share links.
- If sharing externally, for large volumes of files use secure file transfer (SFTP) as it requires a username and password. You can also have a SharePoint site created with third parties. The third party might have their own secure file sharing and that could be more appropriate. Remember, when sharing files with third parties there should be a contract or NDA in place. If using a third-party sharing tool there should also be a data security questionnaire covering that tool.

What if I Need Help or Guidance?

If you are not sure of the best way to share the files you have contact IT using ServiceNow. The IT team will be able to offer further advice and guidance to make your sharing of files as simple and easy as possible while still being secure.

Doing good together

Appendix

How to Share a Link

- In Teams, OneDrive or SharePoint click on the 3 dots that appear when the file name is in focus as below:

- One of the options will be ‘Copy Link’. Select the option.
- Do not accept the default option but select Settings.
- Select ‘People you choose’ so you can select individuals to share the file with.
- Enter the individuals names you wish to share the file with.
- Set whether the file s ‘Can View’ only or one of the other options.
- Set an expiration date as the last option so the file is no longer accessible after the required time.
- Click Apply
- Click Copy Link or Email the link directly.