

## Sharing Data Key Guidance

### Key Contact

Information Security and Risk Manager – Sheridan Hindle  
Society Data Protection inbox - [Data-Protection@midcounties.coop](mailto: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.