



Data protection options available to researchers

Points to note:

- Ø Security is higher on college network servers / shared drives.
- Ø Staff are advised to save files to personal folders on the College P Drive or other shared network folders, as only those with permission to do so can access the folders.
- Ø Encryption is the only way to secure laptop files. Encryption software is user-friendly, however, there are some limitations to using encrypted files, which users will need to consider e.g. if passwords are lost/forgotten, the document is unrecoverable.
- Ø Researchers should be advised to use a pass phrase rather than a password. The pass phrase should be over ten and up to 128 characters long. The longer the pass phrase, the more secure the file. Researchers may have to keep the pass phrase as a separate file, which creates its own problems.
- Ø Researchers are advised to keep a master file of their work on the P or shared drive then copy to their laptop and encrypt individual files. By keeping a master file on the shared drive, the user retains a secure back-up of the file.