**File security plan**

The following methods will be applied to ensure that all files are kept safe and out of the hands of unauthorised parties.

1. Physical security

* Files that contain sensitive data will not be open or displayed when people without permission to view the files are around.
* Laptop will not be left at school overnight.
* Laptop will not be left unattended.
* Laptop will be kept out of sight when unattended, whether in a bag, locker, or other location.

1. Software security

* All files will be stored on the OneDrive cloud service. A very strong password that is not used for any other services will be used. Along with two-factor-authentication to prevent unauthorised parties from accessing data.
* Laptop will not be left unlocked and open before leaving it unattended.
* Unauthorised parties will not be allowed to access files on the laptop. This includes any other users of the laptop which will be signed into a guest account that cannot open these files.
* Files will not be downloaded from non-trustworthy locations to limit potential viruses from being downloaded. And any connections will be through a firewall to limit unwanted downloads from websites.
* The inbuilt MacOS anti-virus software will be used to further ensure safety against viruses.