**File management plan – Syed Naqvi**

To ensure that all files are organised and easy to locate, the following file management plan has been applied:

1. **File naming strategy**

* All files will need to accessible on any macOS device. For this reason, file names will consist of capital and lower case letters, numbers and common symbols.
* Therefore, this approach ensures that the files can be easily located and accessed on any macOS device

A screenshot of a computer

Description automatically generated

Maintains a combination of numbers, upper- and lower-case letters.

* All file names will remain short yet informative, and not exceed a 50-character limit.

A screenshot of a computer

Description automatically generated

Characters do not exceed over 50.

* All file names will use the snake case convention, meaning no spaces will be left in between words. Spaces will be replaced with and underscore (\_) between each word, other than the first.

A screenshot of a computer

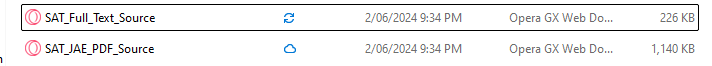
Description automatically generated

Spaces are replaced with an underscore between each word.

* Each primary and secondary data source, such as images, websites, and surveys, will be assigned a unique code and accompanied by a concise three-word summary that describes its intended purpose or goal. For example, Adobe PDF files will be represented by the abbreviation "PDF," followed by the file name in snake case format.

A close up of a number

Description automatically generated



The secondary sources files and pdfs have been assigned a three-letter summary alongside following a snake case format.

* One example of a primary data source adhering to the file management plan is the survey. Following a snake case format; “EXL\_Greatest\_Basketball\_Player”

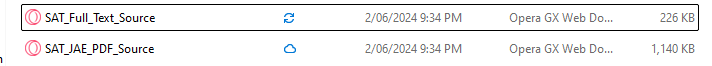


A primary source adhering to snake case format

* Consistent Formatting: Ensure consistency in file naming conventions across all files to facilitate easy navigation and identification. This includes maintaining the same structure for all file names.

A screenshot of a computer

Description automatically generated



Snake case has been implemented in all of the file names

* Secondary sources like websites will be cited using APA referencing within a Word document to ensure organisation and centralise all secondary source links.

A black background with white text

Description automatically generated

A black background with white text

Description automatically generated

Sources have been cited using apa referencing within a word document.

1. **Folder hierarchy and naming strategy**

* Each folder will have a short yet descriptive name that represents the files stored inside. Through the implementation of Snake case and Capital letters at the start of every word, with the 3 letter summary being in all capital.

A group of blue clouds

Description automatically generated

Each folder includes implementation of snake case, 3 word summary and capital letters.

* There will be a maximum of 5 levels of nested folders to improve searchability. This will be done by having the parent folder labelled as “SHL\_Overnewton\_Data\_analytics”, in there it will save to “SHL\_Data\_SAT” (because that is the SAT of research, SHL standing for school) and then be organised into the types of data it represents such as primary or secondary e.g.: “SAT\_Primary\_Sources”, and either word doc or PDF from there.
* 
* A blue and white clouds

  Description automatically generated
* 

There are 3 root nested folders for each main folder.

* An archive folder will be used to store old files that are no longer in use but might be kept for reference.
* 
* There will be a check to ensure that folders are not redundant or repetitive. Each folder should serve a distinct purpose and contain files that are relevant to that purpose.

Each folder has a distinction and its own use.

**File security plan – Syed Naqvi**

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

**Physical Security:**

* Files stored locally or on the cloud on laptop will not be displayed when unknown people are around. To ensure confidential data is not breached and therefore adhere to privacy and human rights laws.

A screenshot of a computer

Description automatically generated files are stored on one drive

* Laptop / Personal computer will not be left at school overnight. ensures that it remains in your possession and reduces the risk of unauthorised access or theft while it is unattended.

Laptop is at home and does not stay in school

* Laptop / Personal computer will be stored in bedroom or wardrobe and not left out in plain sight of others adding an extra layer of protection, ensuring confidential data is not breached and all privacy laws are followed.

Laptop is at home and is hidden away in a drawer or wardrobe

* The survey will track its last access, enabling to determine whether a potential data breach has occurred or not.
* In the event of the laptop being stolen, protocols for handling sensitive data will be initiated. This includes accessing the files stored on OneDrive and deleting any confidential information to prevent unauthorised access.

Protocols such as moving files away and deleting information have been added.

* Computers stored within the household will remain within sight of family members and will be overseen by individuals without access privileges.

When away from home and laptop remains, family members keep watch in case of emergency.

* Access to the laptop and computer will be restricted to authorised users only.

Password only the authorised user knowns is implemented, deterring unauthorised users.

**Software security:**

* All data will be securely stored on the OneDrive cloud service. Security measures, including a highly complex password and two-factor authentication, will be enforced to prevent unauthorised access. Furthermore, every interaction with the cloud service will be meticulously logged with timestamps, enabling the identification of any unauthorised access attempts. Improving data software security.

A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated files are stored in onedrive with a date modification system to determine when these files have been open.

* Laptop will always be locked before leaving it to ensure that unauthorised parties are not able to access files when I am not around.

Laptop is never left open and is locked with a password.

* A guest account will be created on laptop for others who may need to use device. They will not have access to files

No other users have accessed the laptop, but a guest profile has been made on the computer for users when they need to use the device.

* A firewall will be enabled on the laptop to monitor and control incoming and outgoing network traffic. This helps to prevent unauthorised access to the laptop and provides an additional barrier against malware and other malicious activities.
* The computer has a login password consisting of more than 12 characters including different numbers, symbols, and lower and Capital case letters. This ensures the device is protected and all data sourced is safe and encrypted.

A password over 12 letters has been implemented.

* The only person accessing the data is the owner, meaning no user training is required.

No additional user or training is required.

* All data and folders are backed up on OneDrive. In case of a computer malfunction, all data is securely stored in a protected system managed by Overnewton Anglican Community College.

A screenshot of a chat

Description automatically generated All files are backed up in the over newton one drive.

* Regular updates are made to the security system with the latest security patches. This helps to mitigate potential vulnerabilities that could be exploited by attackers.

A screenshot of a computer

Description automatically generated

Updates have been made to mitigate any vulnerabilities.