Data Security

For Employee

(Day to Day Operation)

Devices

Ensure software is updated to prevent malicious activities and for faster processing of information

Strive to use passwords with 12 characters, combination of upper and lower case letters, numbers and symbols

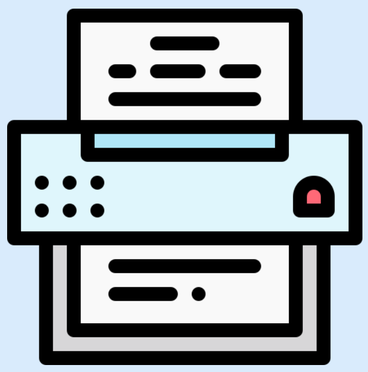
Only use **trusted and secured Wifi** networks with WPA2* encryption (*a form of Wifi encryption that uses a unique identity for your device to connect to the router after you enter the password once)

Ensure laptop and portable devices are properly stored

Safe-keep password and do not share password

Protection of Client Data

Only disclose information for intended purpose
Do not send client's information without consent



Proper storage for client's data

For Organisation
(Management)

Awareness

Increase staff awareness on data security
Eg. Agency's policies and case studies on non-compliance

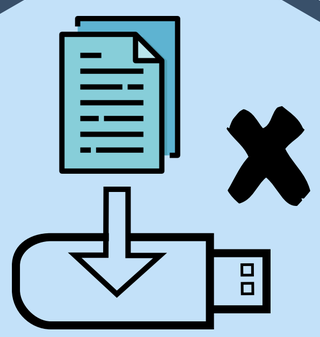
Include information on data management in new staff induction programme
Eg. Email confidentiality, IT Devices Management

Storage

Data Classification
Consider classifying information such that sensitive information is only accessible to the relevant staff

Consider using hardware **encrypted thumb drives**/ thumb drives with in-built software-based encryption

Declaration



Use Confidentiality undertaking
Eg. Not copying client's data into thumb drive

Use Non-disclosure Agreement
Social work data not to be shared with others unless consent is given, or during an emergency

Use

Have access controls
Eg. password securing actions for client database, temporary staff/ students

Use **updated Anti-virus software** and scan portable storage devices and computer regularly

Install strong firewall as a security measure to block unauthorised connections

Protection

Report any suspicious activity immediately

Have frequent review of IT security