Remote Web Access - Data Protection Guidelines

The following guidelines will help you to keep your data safe when accessing it remotely.

1. Never share usernames or passwords.
2. Do not save usernames or passwords on public or shared computers.
3. Passwords must be strong. A strong password will contain a mixture of lower and upper case letters, numbers and symbols. It should not be like your name, username, friends' or family members' names. It should not be a dictionary word, a common name or a keyboard pattern (e.g 12345 or qwerty). It should be at least 8 characters in length: the greater the length the greater the security.
4. Sign out of the Remote Web Access session when you have finished, rather than just closing the web page.
5. If you believe that your user credentials have been compromised, report this immediately and change your password as soon as possible.
6. Do not print out sensitive or personal data to a local printer from a remote access session
7. Do not save sensitive or personal data to a local PC or other storage device from a remote access session, unless you are using a school supplied encrypted laptop or encrypted storage device.
8. Devices used to connect must be fully up to date in terms of windows and other software updates and anti-virus software

Last updated: 26-06-2019.