Patient GP Online Access Security Leaflet

Patient’s responsibility to maintain the security of their online access

The security of online access to GP practice services and records is very important and it is the patient’s responsibility to maintain it. To achieve this, they should:

- Protect their login details so that nobody else can gain access to their record.

- Passwords should be easy to remember or stored in a safe place, such as an encrypted password app. They should not be based on something that is easy to guess.

- If they lose the details or suspect that someone else has seen them, they should change their password immediately and inform the practice.

- Use a password, PIN or fingerprint or face recognition system to protect access to the phone, tablet or computer that they use to access their GP Online Services.

- Log out of their browser when they have finished using online access, especially if they have used a public computer.

- Ensure that nobody can see their record on the screen over their shoulder while they are accessing their GP online account.

- Take precautions to avoid cyber-attacks, using antivirus software, an effective firewall and safe internet browsing whenever possible.

- They must keep and dispose of all information from the record that they download securely.

- People with visual impairment, who use audio electronic readers need to be careful to avoid being overheard, especially in public places.