ICT (inc social media) Guidelines

These guidelines should be followed at all times:

The following ICT Guidelines include use of email, internet, smart phones, tablets and **social networking sites**

a. All faults must be reported to the ICT support officer using the ICT work request form

b. Always keep your password/s secure and ensure they are logged on the password control card and inform the ICT Support Officer if this changes

c. You must not use the Internet or email facilities to circulate information that is confidential to the PCP or its service users

d. All external storage devices (i.e. memory sticks, CD's etc) must be scanned by anti-virus software before use on PCP's hardware. (see ICT for how to guide)

e. All files must be stored on the shared drive (s:) or your personal drive (u:)

f. Always lock your PC before leaving your computer for any periods of time and turn off the monitor

g. Software must not be installed onto any of PCP's hardware unless authorised by the ICT support officer or Operations Manager.

h. Emails to external recipients should include the standard PCP Disclaimer along with the corporate footer

i. If you are away from the office for a significant period of time / annual leave please arrange for an out of office message to be added

j. You must only access the Internet for personal use during your breaks unless specifically authorised by your line manager (including accessing social media) via PC, tablet or mobile phone.

k. Please ensure that your PC and monitor are turned off and switched off at the wall at the end of each working day

l. Adhering to this policy is mandatory and forms part of the Terms & Conditions of Employment, failure to comply with these guidelines may result in disciplinary action being taken

m. Social media updates relating to PCP should carry a disclaimer regarding personal views unless you are expressly authorised to post official updates.