INTERNET AND EMAIL POLICY

E-mail and Internet use creates the possibility of:

- Breaches to the security of confidential information
- Contamination to the system via viruses or spyware

Spyware allows unauthorised people, from outside the practice, potential access to Practice passwords and other confidential information. All staff and practitioners are required to exercise vigilance at all times.

During office hours, e-mail and internet usage is to occur only for work-related purposes and in circumstances where it is necessary for the performance of an employee's duties.

Usage of e-mail or the internet may occur for personal use in the employee's own time, for example, at lunch or before or after work.

However, all staff and doctors should be aware that any electronic communication, its storage or access should not be considered private if it is created or stored at work on Pro Health Care equipment.

Under no circumstances may Pro Health Care computers or other electronic equipment be used to obtain, view or reach any pornographic, or otherwise immoral, unethical, or discriminatory Internet sites. Doing so can lead to disciplinary action up to and including termination of employment.

E-mails sent from the practice to anyone at all which might be construed as offensive, discriminatory or sexually harassing, are not permitted, regardless of whether the transfer occurs during paid working hours or on the employee's own time. If such material is received it is to be completely deleted immediately.

Confidential information must not be shared outside the surgery, without authorisation, at any time.

Procedures for the safe use of e-mail and the Internet

1. **Protection against viruses**
    - Install and use antivirus software
    - Keep antivirus software active at all times
    - Keep antivirus software up-to-date by using automatic updates
    - Periodically, manually check that antivirus software is up-to-date
    - Apply patches to operating and application programmes following technical advice
    - Do not download or open and e-mail attachments where the send is not personally known to you
    - Do not open unexpected e-mail even from people known to you as this may have been spread by a virus
    - Use meaningful and identifying descriptions in the Subject line of e-mails
    - Do not open *.exe or *.bat attachments
    - Use an antivirus mail filter to screen e-mails prior to downloading

- Do not use 'preview' in the e-mail programme as this automatically opens the e-mail when you click on the header
- Save attachments and check for viruses before opening or executing them
- Do not run programmes directly from websites. Download files and check them for viruses first
- Enable security settings in your Internet browser to medium or high

2. Protection against the theft of information

- Do not provide confidential information by e-mail
- Use a second, non-critical e-mail address when registering personal details where you are not completely sure of the site's security
- Do not inform people of your e-mail password

3. Protection against hackers

- Install hardware and/or software firewalls between computers and the Internet
- Test the firewall periodically and update as required
- Do not use a wireless network within the Practice

4. Protection against spam

- Do not reply to spam mail
- Never try to unsubscribe from spam sites
- Do not provide confidential information to an e-mail, especially by return e-mail, not matter how credible the sender's e-mail address seems
- Use a spam filtering programme

5. Protection against spyware

- Learn how to recognise (and delete) spyware
- Do not accept certificates or downloads from suspect sites
- Maintain anti-spyware software

6. Encryption of patient information

- Do not send patient information or other confidential data via e-mail unless you are using encryption
- Encrypted files are not automatically checked for viruses. They must be saved, decrypted and then scanned for viruses before being opened

7. Backing up e-mail and Internet Favourites or bookmarks

- If you rely on information held in your e-mail programme make sure that it is backed up with the rest of your data
- If you have a useful list of Internet Favourites or bookmarks make a back-up of the list. To print a list of the displayed names of the Favourites, as well as the actual links: Open the list of Favourites, go to File/Import and Export. Click Next, select Export Favourites, and save the html file to a file location e.g. W: Shared Work. Go to this location and open the file. Select File/Print, click on the Options tab and put a tick against “Print table of links”.