

Rivermead Gate Medical Centre

COMPUTER SECURITY POLICY (Staff)

Document date: October 2015

Review date: February 2019

Expiry date: February 2021

Version: V01.2

1. Desk Top Computer System

You must log out of the system and switch off your computer at the end of your working day.

A back up must be performed at the end of the day in accordance with the appropriate procedures.

You must not store your user ID and password or authentication device near to your computer. Once security card readers are introduced they must not be given to another member of staff to access the system. They must be stored in a secure place when not in use.

Once smart cards are introduced they must not be given to any other members of staff to access the computer system. The cards must be kept in a safe place away from the computer.

No software can be installed onto the computer without approval from the Practice Manager.

2. User ID / password

You must use your ID and password to access the computer network.

You must keep your password secret and never disclose them to anyone.

Your user ID / password is for your exclusive use. You must not share it or lend it to anyone else.

If you are signed on to a PC and you are going to leave it unattended for any time, you must activate a lock by pressing F11 so that a password is needed to resume work.

3. Virus protection

For protection, the latest anti-virus software will be installed onto the computer network. You must not remove this software yourself.

If the anti-virus software detects a possible virus, an on-screen warning message will be displayed. If you see this message you must report it to the Computer Manager immediately. Do not attempt to remove the virus and do not panic!

If the anti-virus software detects a possible virus and you can not report it immediately to the Computer Manager, turn off the PC and **do not use it again until the problem has been investigated by the Practice Manager.**

If you suspect that a virus has bypassed the anti-virus software on your PC, report it immediately to the Practice Manager. **Do not use the PC again until the Computer Manager gives you the go ahead.**

Rivermead Gate Medical Centre

You must virus check any files created outside the surgery's control, particularly files/data from the internet, before you load and open them onto your PC.

If the Practice Manager is not available or in the case of absence in the first instance call the audit clerk who will contact the Mid Essex IT service desk on 0300 123 1020 for assistance.

4. E-Mail

E-Mail messages (internal and external) should be treated with the same care as traditional written communications. Any messages sent to other NHS Agencies etc. could be seen to represent the views and opinions of the whole practice.

All messages must be written on a professional manner with appropriate language and content. In particular, they must not contain any personal, untrue or defamatory statements about any individual within the surgery.

Because the Internet and e-mail transmissions are not always secure, you must not use them to send confidential or 'surgery' sensitive information to anyone other than those verified by the Practice Manager. If you are in doubt as to whether information is confidential or not, please seek guidance from the Practice Manager.

If you receive an e-mail message that contains material that is inappropriate you must delete it immediately. Under no circumstances should such mail be forwarded to another individual or stored on surgery computers. Inappropriate material includes words or pictures that could be considered obscene, offensive, defamatory or illegal, chain mail, jokes, hate speech, pornography and messages which are inconsistent with government legislation, i.e. equal opportunity, race and harassment policies. This list is illustrative, BUT NOT EXHAUSTIVE.

All e-mails are liable to be intercepted. Where inappropriate messages originate from within the surgery, disciplinary action will be taken.

Where an intercepted e-mail is attempting to come into our system, then we will endeavor to identify the sender. Where the e-mail has come from another surgery/company, the surgery/company will be informed of the identity of the individual and the nature of the e-mail.

The dissemination of inappropriate material is strictly forbidden. It may result in dismissal and may also constitute a criminal offence.

If you receive an offensive message, you must report the incident to the Practice Manager.

In cases of obscene and offensive e-mails, the information will be passed onto the Police for possible prosecution.

5. Internet

You must not download programs from the Internet without permission from the Practice Manager.

Use of the Internet will be monitored. In instances where the monitoring identifies the Internet Policy has been contravened, disciplinary action will be taken.

Where accessing the Internet employees should act in a 'responsible manner'. Whatever applies in spirit to use of e-mail as described in Section 4 also applies to the Internet.

Rivermead Gate Medical Centre

Users must not access inappropriate or offensive Internet sites that are related to gambling, pornography, jokes, criminal skills, terrorism, cults, hate speech, illegal drugs, chain mail or anything not related to work issues. This list is illustrative, NOT EXHAUSTIVE. Failure to comply may result in dismissal and may also constitute a criminal offence.

6. Auditing

The surgery has the right at any time to audit any surgery property, be it a PC, portable computer, terminal, disk drive, e-mail or paper. If there is evidence that the policy set out in this document has been contravened, the employee concerned may be subject to disciplinary procedures which could include dismissal. Any evidence that an employee has committed a criminal offence may be forwarded to the appropriate authorities for further action.

I, the undersigned, have read and therefore acknowledged the content of this document.

Signed: Dated:

Print name:

(Please return the signed copy of this document to the Practice Manager and keep the other copy in a safe place for your reference).