



E-MAIL AND INTERNET POLICY

1. Introduction

- 1.1 The Trust recognises that electronic communication systems and equipment are intended to promote effective communication and working practices, and are critical to the success of the Trust. This policy sets out the standards the Trust requires all users of these systems and equipment to observe and the circumstances in which we will monitor use of these systems and equipment. Failure to comply with this policy will constitute a disciplinary offence and will be dealt with under the Trust's Disciplinary and Dismissal Procedure.
- 1.2 This policy applies to all individuals working at all levels of the Trust, including senior managers, officers, directors, employees, consultants, contractors, trainees, home workers, part-time and fixed-term workers, casual and agency staff, and volunteers (collectively referred to as **staff** in this policy).
- 1.3 This Email and Internet Policy does not form part of any employee's contract of employment and is entirely non-contractual. It may be amended, withdrawn, suspended or departed from at the discretion of the Trust.

2. Property

Staff should treat any property belonging to the Trust with respect and reasonable care and report any faults or breakages immediately to the Technical Services Manager. Staff should not use the Trust's computers unless you are competent to do so and should ask for training if you need it.

3. Viruses

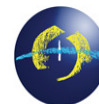
Staff should be aware of the potential damage that can be caused by computer viruses. Staff must not introduce or operate any programmes or data (including computer games) or open suspicious e-mails which have not first been checked by the Trust for viruses.

4. Passwords

Passwords protect the Trust's network and computer system. They should not be obvious, for example a family name or birthdays. Staff should not let anyone else know their password. If staff believe that someone knows your password staff must change it immediately. Staff should not attempt to gain unauthorised access to anyone else's computer or to confidential information which they are not authorised to access.

5. Leaving workstations

If staff leave their workstation for any period of time they should take appropriate action and, in particular, should log off and/or set their screen saver with an appropriate password.



6. Systems and Data Security

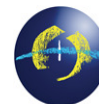
- 6.1 Staff should ensure that they do not delete, destroy or modify any existing systems, programs, information or data which could have the effect of harming or exposing the Trust to risk.

7. Internet

- 7.1 **Misuse:** The Trust recognises that for some staff, use of the internet is an integral part of their duties or function. The internet facility is provided for Trust related activities only. The Trust monitors the use of the internet. If it discovers its use has been abused or is contrary to this policy, disciplinary action may be taken, under the Trust's Disciplinary and Dismissal Procedure for employees or if the member of staff is not an employee, the ending of any agreement or contract with the Trust.
- 7.2 **Downloading:** Downloading of any programme or file which is not specifically related to your duties or function is strictly prohibited.
- 7.3 **Personal use:** Use of the internet during working hours for personal reasons is discouraged. If the Trust discovers that excessive periods of time have been spent on the internet provided by the Trust either in or outside working hours, appropriate disciplinary action may be taken, under the Trust's Disciplinary and Dismissal Procedure for employees or if the member of staff is not an employee, the ending of any agreement or contract with the Trust.
- 7.4 **Unsuitable material:** Viewing, retrieving or downloading of pornographic material, or any other material which the Trust believes is unsuitable, at any time, is strictly prohibited and constitutes gross misconduct. Internet access may be withdrawn without notice at the discretion of the Trust whilst allegations of unsuitable use are investigated by the Trust.
- 7.5. **Contracts:** Staff are not permitted to enter into any contract or subscription on the internet on behalf the Trust, without specific permission from your College Management Team or Director of a Directorate.

8. E-mail

- 8.1 **Personal use:** E-mail is provided for Trust related purposes only and personal use is discouraged. Staff should only give their allocated e-mail address where their duties or function requires. The Trust monitors the use of e-mail.
- 8.2 **Status:** Staff should consider whether e-mail is the most appropriate means of communication and any e-mail should be treated in the same way as any other form of written communication. Staff should not include anything in an e-mail which is not appropriate to be published generally.
- 8.3 **Checking of E-mails:** Staffs should access their e-mails on at least one occasion during every working week, including when they are at a remote location.



- 8.4 **Inappropriate use:** Any e-mail message which is abusive, discriminatory on grounds of sex, marital or civil partnership status, race, disability, sexual orientation, religious belief or age or defamatory is not permitted. Use of the e-mail system in this way constitutes gross misconduct. The Trust will take no responsibility for any offence caused by you as a result of downloading, viewing or forwarding inappropriate e-mails.
- 8.5 **Legal proceedings:** Staff should be aware that e-mails are disclosable as evidence in court proceedings and even if they are deleted, a copy may exist on a back-up system or other storage area.
- 8.6 **Jokes:** Trivial messages and jokes should not be sent or forwarded to the e-mail system. Not only could these cause distress to recipients (if inappropriate) but could also cause the Trust's IT system to suffer delays and/or damage.
- 8.7 **Contracts:** Contractual commitments via an e-mail correspondence are not allowed without prior authorisation of a member of your College Management Team or the Director of a Directorate.
- 8.8 **Disclaimer:** All correspondence by e-mail should contain the Trust's disclaimer. Details are available from the Technical Services Manager.
- 8.9 **Monitoring:** The Trust regularly monitors the use of the internet and e-mail systems to check that the use is for work-related purposes. If it is discovered that any of the systems are being abused and/or that the terms of this policy are being infringed, disciplinary action may be taken which could result in your dismissal.
9. **Where to get help**
- 9.1 Any concerns or queries that arise out of this policy should be directed in the first instance to a member of the Technical Services Team or a member of the appropriate College Management Team or the appropriate Director of a Directorate.