South East Coast Ambulance Service NHS
NHS Foundation Trust

Internet and Email Policy

Contents

1. Statement of Aims and Objectives

1.1. This policy identifies the arrangements for managing internet and email access and provides assurance on the acceptable and safe use of these facilities by staff.

1.2. This policy governs the use of the Internet and Email connected systems and is designed to ensure staff do not breach any NHS policies regarding Internet / Email use or inadvertently breach any other associated guidance or legislation, i.e. the Data Protection Act 2018; the General Data Protection Regulation (GDPR) 2016; the Human Rights Act 1998; the Computer Misuse Act 1990 and current legislation relating to discrimination, harassment, defamation and pornography.

1.3. Principles included in this policy apply to all forms of communication using Trust provided tools, as well as using non-Trust equipment to access Trust systems or services, **including but not limited to:**

- Browser software such as Workspace One Secure Browser, Chrome, Safari and Edge.
- Email software clients such as Microsoft Outlook and mobile device native email applications.
- Instant messaging and video conferencing applications including, but not limited to, Microsoft Teams and Teams Video Conferencing platforms or FaceTime.
- Tablet devices such as Apple iPads, Android Tablets and Microsoft Surface Pro.
- Mobile telephones and smartphones, mobile instant message applications and text messaging.

1.4. **This policy aims to ensure:**

- Staff are aware of what is and is not acceptable use of Internet and email facilities.
- Equity of access to those facilities for those staff that need it to perform their job.
- Staff are aware that their usage of Internet and email facilities is subject to reactive monitoring and may be recorded.
- Records of activity relating to the use of Trust Internet and email facilities are not considered to be personal information.
- Monitoring reports will constitute evidence of user activity and be provided to appropriate line managers on request, where available.

1.5. **Acceptable use of Trust provided mobile devices is addressed in the following policies:**

- Mobile Device Policy.
- Removable Media Information Security Policy.
- Information Governance Policy.
- Patient Photographic and Video Recording Policy.

1.6. Cloud Services, Refer to NHS Digital guidance contained in: NHS and social care data: off-shoring and the use of public cloud services (https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services). This National guidance has been published setting clear expectations for health and care organisations who want to use cloud services or data offshoring to store patient information.

2. Principles

2.1. Provision of Internet Access

2.1.1. Internet access will be provided for staff that have an active Trust network account from all Trust sites. **Accounts are requested by:**

- Provision and processing of a starters list from Human Resources.
- Directly from line management to IT via the IT Service Desk.
- Directly from a member of staff via the IT Service Desk and validated by IT through appropriate line management.

2.1.2. The IT Service Desk will allocate an individual user login and password enabling access to internet and email facilities.

2.1.3. Use of the supplied username and password implies acceptance of the terms set out in this policy.

2.1.4. The Trust has Internet facilities that are available to staff and agents acting on behalf of the Trust to use for business purposes. These terms and conditions apply to any staff or agents acting on behalf of the Trust and those members of staff who use stand-alone and/or non-Trust provided devices for accessing the Internet.

2.1.5. Where a third party requires Internet access for partnership working, contractual or demonstration purposes, a member of Trust staff must make the request to the IT Service Desk on their behalf.

2.1.6. Third party access will be provided on a case by case basis and the requesting member of staff will be required to monitor and be responsible for the third parties use of Trust facilities.

2.1.7. Third party Internet activity will be subject to reactive monitoring and by request of the responsible member of staff.

2.1.8. Only hardware supplied or owned by the Trust may be connected to a Trust network.

2.1.9. Personally owned or third party hardware can be connected to isolated or Internet-only connected networks, such as the Trust Guest WIFI, where appropriately provided by IT.

2.1.10. Where agile working has been approved by line management, staff can connect their Trust provided mobile devices to home broadband.

2.2. **All users (staff and agents) of these facilities must abide by the conditions detailed below:**

- Access is granted only in accordance with this policy. Any member of staff or an agent of the Trust who may be found to be misusing the Internet facilities may be subject to disciplinary and/or legal action.

- Internet facilities are to be used for business purposes and any personal use of these facilities must be kept to a minimum unless a Corporately Owned Personally Enabled (COPE) device has been issued (see below).

- Reasonable personal use is subject to local management arrangements or as specified by other relevant policy or procedure.

2.2.1. Removal of Internet access privileges will be considered on a case by case basis and applied only as a last resort where management has been unable to address significant risk and the decision is supported by Human Resources.

2.3. **Corporately Owned Personally Enabled (COPE)**

2.3.1. COPE devices are issued specifically for combined corporate and personal use and limited to Trust provided iPads and smartphones.

2.3.2. COPE devices are controlled using Mobile Device Management software which logically splits and secures personal and corporate applications and data.

2.4. **Appropriate Use of Internet Facilities**

2.4.1. **The use of Internet and email facilities for any of the purposes listed below is not considered acceptable use and may be subject to disciplinary action and/or prosecution:**

- Accessing and/or transmitting immoral language and/or images, promoting violence, incitement to criminal behaviour, racial/religious discrimination on the basis of any protected characteristics (such as race or religion) or sexual harassment.

- Transmitting content that is defamatory or with the intent of being offensive, making anyone uncomfortable, bullying, harassing or intimidating.

- Accessing and/or transmitting content likely to bring the Trust into disrepute or committing a criminal offence.

- Accessing and/or transmitting pornography or activities which contravene safeguarding policies and practices.

- Activities for personal financial gain such as gambling or performing commercial operations using Trust resources to operate a business from work.

- Fraudulent activity.

- Downloading, storing or using material or media protected by copyright or licensing arrangements whether for personal or business use unless express permission has been given by the copyright owner (Copyright Designs and Patents Act 1988).

2.4.2. Internet monitoring systems implemented by the Trust will automatically block specific websites or functionality based on categories as defined by the manufacturer of those systems.

2.4.3. Social media sites such as Facebook, LinkedIn and Twitter are not actively blocked and reasonable personal use should be subject to local management arrangements, relevant policies and procedures. See COPE definition above.

2.4.4. Specific websites will not be blocked by Trust managed Internet monitoring systems for named individuals or limited staff groups only.

2.5. **Publishing Information on the Internet**

2.5.1. Staff that create or contribute to a web-based site must not create or transmit material that is designed or likely to cause annoyance, inconvenience, needless anxiety; or that may infringe the copyright of another person or bring the Trust into disrepute.

2.5.2. Examples of how the Trust's reputation may be damaged would include posting derogatory remarks about the Trust, its staff, other NHS colleagues, patients or members of the public on social networking or similar sites; discussing incidents on-line or posting photographs or names of individuals without their consent. This list is not exhaustive, and staff must exercise caution when publishing information on the Internet.

2.5.3. The Trust has a Social Media Policy which all staff must abide by whilst accessing such media.

2.5.4. Personal data placed on the Internet is available worldwide. Generally speaking, current Privacy Law - namely the GDPR and Data Protection Act 2018 - govern data protection within the European Economic Area (EEA). There are alternative 'safe countries' which apply, but for the avoidance of doubt any request / requirement to publish personal data must be firstly referred to the Head of Information Governance / Data Protection Officer for review.

2.6. **Downloading Content from the Internet**

2.6.1. Anti-virus and malware detection software is installed on all Trust computers configured to automatically remove or quarantine infected content downloaded from the Internet or email.

2.6.2. This protection cannot be 100% effective and so caution should always be exercised when receiving unexpected content. If you receive an alert or are concerned about any aspect contact the IT Service Desk for advice.

2.6.3. If you are prompted to perform an activity such as calling a telephone number after opening a downloaded or emailed file attachment contact the IT Service Desk for advice.

2.6.4. Person identifiable data must not be copied to unencrypted removable media and staff must contact the IT Service Desk for advice prior to downloading the information.

2.6.5. The loss of person identifiable data could subject the Trust to significant fines and reputational damage and staff could be subject to disciplinary action and/or prosecution.

2.7. **Appropriate Use of Email Facilities**

2.7.1. Email facilities are provided for business purposes only and all content sent and received should not be considered personal or private.

2.7.2. Email content is subject to Trust scrutiny as defined under the terms of the Regulation of Investigatory Powers Act 2000, if breaches of this policy are suspected.

2.7.3. It is prohibited to send inappropriate messages, for instance any that might cause offence or harassment on grounds of the protected characteristics.

2.7.4. Any member of staff or an agent of the Trust who is found to be misusing the email facility may be subject to the Trust's disciplinary procedures and/or prosecution.

2.7.5. Any suspicion of fraud will result in information being shared with the NHS Counter Fraud Service.

2.7.6. Any subsequent investigation may result in Criminal, Civil and/or disciplinary action being taken.

2.7.7. Users should evaluate each email before sending taking into consideration whether the content could be misconstrued by third parties or staff and whether further clarification should be added to avoid misunderstanding. Users should assess the use of 'cc' and 'bcc' when replying to emails to ensure that communication remains between interested parties.

2.7.8. Emails should be written with care. They are regarded as business records and may be required in connection with future disputes and/or litigation and may also be subject to disclosure under the Freedom of Information Act 2000 and/or Data Protection Act 2018 and/or General Data Protection Regulation (GDPR) 2016. All Emails remain the property of the Trust.

2.7.9. Whilst emails can be deleted by staff, all email content is regularly backed up and may be restored for the purposes of audit, Data Subject Access Requests or in response to 2.7.8 above.

2.7.10. Staff are responsible for the use of their email account and should ensure access is provided only where necessary and passwords are not shared with other staff, friends or family.

2.7.11. **Trust email accounts must not be used for:**

- Sending broadcast communications to large numbers of recipients. Staff should address their requirement with the Communications department first who may send it on their behalf.
- Selling personal items, opportunities or services.
- Canvassing opinion or expressing political views not related to Trust activities.

2.8. **Accessing another member of staff's email account**

2.8.1. Requests to access another member of staff's mailbox can only be authorised, in writing, by the mailbox owner or by an Executive Director or their nominated Deputy.

2.8.2. If the access request relates to the mailbox of a staff member still employed with the Trust, a notice period of 5 working days must be given before access is granted to an approved individual.

2.8.3. If the access request relates to the mailbox of a staff member no longer with the Trust approval must still be granted in line with 2.8.2 above but the 5-day notice period will not apply.

2.8.4. For confidential emails, staff are reminded to put the words "CONFIDENTIAL ADDRESSEE ONLY" in the subject line and to set the Outlook Sensitivity Tag to Confidential.

2.8.5. Employees that have been granted access to another staff member's mailbox must not open any emails with CONFIDENTIAL ADDRESSEE ONLY in the subject line without the written approval of an Executive Director or their nominated Deputy.

2.9. **Confidential or Sensitive Information**

2.9.1. The Trust has met the NHS security standards and has given the Trust secure email accreditation which will allow for person identifiable or sensitive data to be sent via email.

2.9.2. Confidential or sensitive information can also include information relating to the Trust's affairs that have been restricted from general use. These sensitive documents may or may not be marked as 'restricted' but will imply their confidential nature by their contents.

2.10. **Reporting of Serious Incidents**

2.10.1. In the event of a serious breach occurring, whether deliberate or accidental, the incident must be reported to the Associate Director of IT (or their representative) by phone or email in the first instance. This should then be followed by the completion of an Incident Reporting Form DIF1 as described in the Incident Reporting Policy & Procedure.

2.10.2. The Associate Director of IT or Head of IT Infrastructure & Networks will validate the breach and notify the Head of Information Governance and the Executive Director of Finance of actions to be carried out where required.

3. Responsibilities

3.1. The Chief Executive Officer (CEO) is ultimately accountable for the implementation of this Policy.

3.2. The Trust Board have responsibility to obtain assurance that the processes described work effectively and support the Board level public commitment to implementation of the Internet and Email Policy.

3.3. The Executive Director of Finance has delegated responsibility to ensure compliance with the Internet and Email Policy. The Executive Director of Finance will report to the Trust Board and the CEO on matters relating to this Policy.

3.4. The Associate Director of IT has overall management responsibility of this policy.

3.5. The Head of IT Infrastructure & Networks will ensure the implementation of this policy.

3.6. The Head of IT Service Delivery will ensure all computers are configured to direct Internet and email traffic through the appropriate monitoring systems.

3.7. IT Support Engineers and IT Security Staff will regularly check usage logs and inform line managers and IT management of any heavy or inappropriate usage where detected.

3.8. The Information Governance Working Group (IGWG) will monitor any non-conformances reported to them by the Associate Director of IT or Head of Information Governance.

4. Staff Responsibilities

4.1. All employees are given permissions to undertake their responsibilities of employment by use of Internet and email systems at any point of access available to the Trust.

4.2. Use of the Internet is permitted and encouraged where such use is suitable for ‘business, training and education’ purposes and supports the Trust’s objectives. The Internet is to be used in a manner that is consistent with the Trust’s standards of conduct and values and as part of the normal role of an employee’s job responsibilities.

4.3. Staff using Internet facilities must be aware that each site they visit is recorded automatically by monitoring software. All users of the Internet must abide by the

conditions detailed within this policy. Any user found repeatedly attempting to access inappropriate sites and/or breaching this policy may face disciplinary action that could lead to dismissal and/or legal action.

4.4. All staff are responsible for information security and therefore must understand and comply with Trust policy and associated guidance. Failure to do so may result in disciplinary action.

4.5. In particular, **all staff should understand:**

- What information they are using, how it should be protectively handled, stored and transferred.
- What procedures, standards and protocols exist for the sharing of information with others.
- How to report a suspected beach of information security within the organisation.
- Their responsibility for raising any information security concerns with the Associate Director of IT or Head of IT Infrastructure & Networks.

5. Competence

5.1. All users will be expected to use the computer systems in the areas of their responsibility and will be made aware of appropriate direction by line management. In addition, the IT department will give appropriate instructions at the point of handover of any computer system being used by them.

6. Monitoring

6.1. Inappropriate Use

6.1.1. Potential inappropriate uses are automatically recorded, and logs are monitored regularly by the IT Security Team.

6.1.2. Where inappropriate use is verified following investigation by IT, the details will be passed to line management and HR for disciplinary consideration.

6.2. Information Governance or Other Issues

6.2.1. All such breaches, whether intentional or otherwise will be reported to the Head of Information Governance.

6.2.2. Monitoring will be undertaken to ensure compliance with this policy.

6.2.3. Monitoring will include the interception of personal electronic communications such as email. This monitoring falls within the remit of the Regulation of Investigatory Powers Act 2000 (RIPA). This generally renders the interception of communications unlawful by non-government organisations without the consent of both the sender and recipient. However, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 recognise that employers need to be able to monitor systems, without seeking individual consent.

6.3. **Internet Monitoring**

6.3.1. Monitoring is managed by a software system that automatically records staff Internet activity and populates management reports.

6.3.2. The Head of IT Infrastructure & Networks reviews the management reports and escalates misuse, in line with this policy, to the IT Manager's Meeting to identify the action to be taken.

6.3.3. When misuse is suspected, in line with this policy, the Head of IT Infrastructure & Networks, or chair of the IT Manager's Meeting, will determine the action to take in reporting the findings to the relevant members of staff or organisations.

6.4. **Email Monitoring**

6.4.1. Emails are not routinely monitored and will only be investigated under circumstances described in section 2.6 above.

6.4.2. When misuse is suspected, in line with this policy, the Head of IT Infrastructure & Networks will determine the action to take in reporting the findings to the relevant members of staff or organisations.

7. Audit and Review

7.1. Audit of all systems is automated by system software and reports are produced weekly.

7.2. The Head of IT Service Delivery is responsible for the review of the reports ensuring any non-conformance against this policy is brought to the attention of other senior IT managers.

7.3. Other audit and review will be undertaken where necessary when the system reports identify non-conformance.

7.4. This document will be reviewed in its entirety every three years or sooner if new legislation, codes of practice or national standards are introduced, or if feedback from employees indicates that the policy is not working effectively.

7.5. All changes made to this policy will go through the governance route for development and approval as set out in the Policy on Policies.

8. References

- Data Protection Act 2018
- General Data Protection Regulation (GDPR) 2016
- Human Rights Act 1998
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Freedom of Information Act 2000

9. Glossary

- **Trust:** South East Coast Ambulance Service NHS Foundation Trust
- **SMS:** Short Message Service
- **IGWG:** Information Governance Working Group
- **ePCR:** electronic Patient Clinical Record

South East Coast Ambulance Service NHS
NHS Foundation Trust

Equality Analysis

The Trust believes in fairness and equality, and values diversity in its role as both a provider of services and as an employer. The Trust aims to provide accessible services that respect the needs of each individual and exclude no-one. It is committed to comply with the Human Rights Act and to meeting the Equality Act 2010, which identifies the following nine protected characteristics: Age, Disability, Race, Religion and Belief, Gender Reassignment, Sexual Orientation, Sex, Marriage and Civil Partnership and Pregnancy and Maternity.

Compliance with the Public Sector Equality Duty: If a contractor carries out functions of a public nature then for the duration of the contract, the contractor or supplier would itself be considered a public authority and have the duty to comply with the equalities duties when carrying out those functions.