Essex Partnership University
NHS Foundation Trust

# EMAIL/INTERNET/INTRANET ACCESS AND USE PROCEDURE

| | |
|---|---|
| **PROCEDURE REFERENCE NUMBER:** | CPG50b |
| **VERSION NUMBER:** | 1.4 |
| **KEY CHANGES FROM PREVIOUS VERSION** | Minor amendment in 9.9 (new bullet) |
| **AUTHOR:** | [redacted] |
| **CONSULTATION GROUPS:** | IGSSC |
| **IMPLEMENTATION DATE:** | May 2018 |
| **AMENDMENT DATE(S):** | February 2019, March 19 (secure email changes); Dec 2019 (review date change); Sept 2020 (minor amendment 9.9) |
| **LAST REVIEW DATE:** | N/A |
| **NEXT REVIEW DATE:** | May 2021 |
| **APPROVAL BY INFORMATION GOVERNANCE STEERING SUB-COMMITTEE:** | March 2018 |
| **RATIFICATION BY QUALITY COMMITTEE:** | May 2018 |
| **COPYRIGHT** |  |

| **PROCEDURE SUMMARY** |
|---|
| These procedural guidelines will ensure that the risk associated with not having a procedural document in relation to information governance / security in regard of email and internet/intranet use is minimised and that there is a co-ordinated approach to the safe use. |
| **The Trust monitors the implementation of and compliance with this procedure in the following ways;** |
| The Information Governance Steering Sub Committee and Quality Committee will have overall responsibility for overseeing the implementation of this policy and its associated procedural guidelines, taking forward any action relating to information governance / security within the Trust. The Information Service Management Team and Information Governance Steering Sub-Committee will be responsible for overseeing the operational implementation of this policy and its associated procedures, as appropriate |

| Services | Applicable | Comments |
|---|---|---|
| Trustwide | ✓ | |

**The Director responsible for monitoring and reviewing this procedure is Executive Chief Finance Officer**

**ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST**

# EMAIL/INTERNET/INTRANET ACCESS AND USE PROCEDURE

## CONTENTS

**THIS IS AN INTERACTIVE CONTENTS LIST – PLEASE CLICK ON THE SECTION HEADINGS TO GO TO THE SECTIONS**

**ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST**

# EMAIL/INTERNET/INTRANET ACCESS AND USE

**Assurance Statement**

These procedural guidelines will ensure that the risk associated with not having a procedural document in relation to information governance / security in regard of email and internet/intranet use is minimised and that there is a co-ordinated approach to the safe use.

## 1.0 INTRODUCTION

1.1 Essex Partnership University NHS Foundation Trust (the Trust) makes extensive use of electronic mail (e-mail) and internet/intranet both within the Trust and with external organisations.

1.2 This document is intended to define in a clear and straight-forward manner the risks and the conditions under which the Trust's e-mail and internet/intranet systems might be used.

## 2.0 AIMS AND OBJECTIVES

2.1 The purpose of this document is to define the procedure for use of the Trust's e-mail and internet/intranet systems. The policy applies to the Trust's employees and others carrying out work on behalf of the Trust.

2.2 This procedure applies equally to basic e-mail messages and to any attachments sent with messages. For ease of reading, the term e-mail is used to refer to both basic messages and to any attachments and other associated files throughout the remainder of this document.

2.3 The purpose of this procedure is to clearly explain what is acceptable and unacceptable when using the Internet/Intranet.

## 3.0 RESPONSIBILITIES

3.1 ***Directors must:-***

- ensure that this procedure is distributed throughout the Trust.

3.2 ***Managers must:-***

- ensure that all of their staff are aware of this procedure and understand their responsibilities under it.
- identify, and provide secure access to equipment that their staff may use to access e-mail and internet/intranet systems.
- ensure that their staff follow this procedure
- Ensure that NHS.mail accounts are cleared of Trust emails on staff leaving EPUT.

3.3 ***Employees must:-***

- make themselves aware of this procedure and follow it whenever they access the internet/intranet.
- only use e-mail systems in accordance with this procedure.
- only access e-mail systems if they have been authorised to do so.
- not share the access privileges that they have been granted with others.
- not use others' access privileges to access e-mail or internet/intranet systems.
- ensure all personal e-mails are deleted from their account when leaving the Trust.
- Staff must not use their personal email for work purposes.
- NHS.mail accounts must be cleared of Trust emails on staff leaving EPUT.

3.4 ***Assistant Director of I.T. Service Delivery must:-***

- ensure the continued management of information technology security.

3.5 ***IT Support Staff must:-***

- only install and give access to the e-mail or internet/intranet systems after the request for access has been authorised.
- record activity by the Trust employees on e-mail or internet/intranet systems.
- regularly review the security effectiveness of the means of access.

## 4.0 DEFINITIONS

4.1 **NHSmail**

- NHSmail should be used to send sensitive/patient/ resident identifiable information by secure (encrypted) e-mail. All staff should have an NHS.mail account.

4.2 **Patient or Residents /Personal Information**

- ***"Personal Data"***

Means any information relation to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

4.3 **Sensitive Personal/Business Information**

- ***"Special categories of personal data"(sensitive) Article 9***

Means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely

identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4.4 **Chat Rooms**

- These are social networking sites such Facebook, Myspace etc. (*Please refer to the Social Media Policy / Procedure for further guidance)*

4.5 **I.P. Address**

- This is the unique address for your computer.

## 5.0 USING E-MAIL SYSTEMS

Only approved Trust enabled email systems can be used or NHS Mail (nhs.net).

***Acceptable Use:-***

5.1 Any e-mail address provided by the Trust, assigned by the Trust to individuals, sub-units, or functions of the Trust, is the property of Essex Partnership University NHS Foundation Trust ('The Trust').

5.2 Those that use Trust email services are expected to do so responsibly, that is, to comply with national laws, with this and other policies and procedures of the Trust, and with normal standards of professional and personal courtesy and conduct.

5.3 Access to Trust e-mail services, when provided, is a privilege that may be wholly or partly restricted by the Trust without prior notice when there is Substantiated Reason to believe that violations of law or policy have taken place, or, in exceptional cases, when required to meet time-dependant, critical operational need.

5.4 As e-mail messages may have to be disclosed in litigation / Freedom of Information requests, it is always good practice for users to ask themselves before sending an e-mail message how they would feel if it was read out in court / released for publication.

5.5 An e-mail message is, for legal purposes, treated as a publication and is therefore subject to all normal legal restrictions on publication.

5.6 E-mail may appear to be informal but can be used to create binding contracts and users must take due care not to enter into contractual obligations without the usual care and attention to detail necessary to protect the Trust's interests.

5.7 Access to e-mail will be inspected and/or monitored by Trust systems to protect the Trust, Trust Computing Facilities and account holders from e-mail borne viruses/macros/inappropriate attachments and/or content where possible.

5.8 All email records destined for the internet will have an email disclaimer appended to the end of the email by the Trust systems. An example below:

*"It is intended solely for the addressee. Please notify the sender immediately if you are not the intended recipient. Access to this email by anyone else is unauthorised. If you are not the intended recipient, any disclosure, copying, distribution or any action taken or omitted to be taken in reliance on it, is prohibited and may be unlawful.*

*Any views expressed in this email are those of the individual, and may not represent the views of Essex Partnership University NHS Foundation Trust.*

*The presence of this disclaimer indicates that the email has been virus scanned. Although this email and any attachments are believed to be free of any virus, or any other defect which might affect any computer or IT system on which they are received and opened, it is the responsibility of the recipient to ensure that they are virus free. Essex Partnership University NHS Foundation Trust accepts no responsibility for any loss or damage arising in any way from receipt or use thereof. If you received this in error, please contact the sender and delete the material from any computer."*

5.9 When sending Patient/ Resident/ Personal/Sensitive Identifiable Information via e-mail all documents must be password protected or sent through NHSmail. Passwords should be forwarded to recipients by telephone or text wherever possible – in emails a suitable gap should be left between the original email and the password to enhance security.

5.10 No Patient/Resident/ Personal/Sensitive Identifiable Information should be listed in the Subject Heading Bar. The subject window of confidential information transferring by email must be identified as "SAFE HAVEN". Best practice requires that no identifiable information is used within the body of the email unless it is absolutely essential in which case initials can be used unless these initials can identify an individual.

5.11 Emails must be checked to ensure that responses / replies are only sent to the relevant recipients and that the content of the email does not include irrelevant email "runs" (additional information included within the email).

5.12 The use of e-mail messages to send patient/resident identifiable data internally within the Trust may be undertaken only to those individuals who are authorised to receive it, when Caldicott principles have been applied and must be encrypted or password protected where possible.

5.13 There are many departments within the Trust that use e-mail as equivalent to an authorised and signed document. Users must be certain of the validity of the content of the mail and its sender before action is taken upon them.

5.14 It is understood that staff sometimes need to deal with personal / private matters during the working day. Limited personal use is therefore allowed provided it is kept to a reasonable level and does not interfere with the working day. This arrangement will be based on trust and all staff will be expected to use this facility in an appropriate manner. Staff should be aware that personal use of e-mail will be monitored.

5.15 The printing of e-mail messages is generally unnecessary. Users should consider developing the habit of dealing with all correspondence electronically, including on-line filing of any messages they wish to retain.

5.16 Data within an e-mail is predominantly confidential Trust data. As such it may be subject to the provision of Data Protection and Freedom of Information legislation.

5.17 E-mail distribution lists must only contain addressees who appropriate recipients of the e-mail content. E-mail **must not** be sent out to a large number of people unless essential as you could be wasting people's time and causing possible disruption to services. Do not ask for acknowledgements from distribution lists.

5.18 If a message is not delivered, you will receive a non-delivery report. This will normally identify the cause of non-delivery such as incorrect address, unavailable end system, etc. Look at this information first before raising a request for support as you may just need to correct the address.

5.19 Delivery reports indicate that the e-mail has been successfully sent and will only be returned if the sender has requested it.

5.20 Receipt notifications indicate that the recipient has opened the e-mail. Remember that the recipient may not have read or acted upon the e-mail, as a personal assistant or administrator may have read the e-mail on behalf of the recipient.

5.21 Delivery reports or read receipt notifications may incur a charge from NHSmail or other service providers, so only request these when you need positive confirmation that a message has been received and read. These types of notifications may not be available from other recipients.

5.22 The following email domains are secure and encrypted;

- nhs.net
- secure.nhs.uk
- gov.uk (no longer needs to be gsi.gov.uk)
- cjsm.net
- pnn.police.uk
- mod.uk
- parliament.uk

***Unacceptable Use:-***

5.23 The Trust shall permit the inspection, monitoring, or disclosure of e-mail without the consent of the account holder if e-mails contain obscene, indecent, racist or illegal content:

- when required by and consistent with law
- when there is Substantiated Reason to believe that violations of law or of Trust Policies have taken place
- when there are Compelling Circumstances
- Under time-dependent, critical operational circumstances as defined in the procedural guidelines (3.0).

5.24 E-mail messages or attachments **not password protected** must not contain any Patient/Resident /Personal/Sensitive Identifiable Information. Sending PID by NHSMail to NHSMail is the most secure method.

5.25 Access to e-mail is provided for staff to use in the course of their work. Staff are prohibited to access, view, download, display or distribute any of the following:

- anything which constitutes pornography
- anything which is sexually explicit
- anything which is libellous
- anything which is sexist, homophobic, racist
- anything which is otherwise offensive.

5.26 Where staff inadvertently access e-mail which may fall into the group above (5.23) this should be reported to the Trust's ITT Helpdesk immediately.

5.27 Trust e-mail services may not be used for:

- unlawful activities
- commercial purposes not under the auspices of the Trust
- personal financial gain
- relaying person identifiable information / data to home email systems for the purposes of working from home unless connected to the Trust networks via the Virtual Private Network (VPN)
- personal use that:
  - directly or indirectly interferes with the Trust operation of computing facilities, internet or email services
  - burdens the Trust with noticeable incremental cost
  - interferes with the user's employment or other obligations to the Trust
  - gives the impression that the user is representing, giving opinions, or otherwise making statements on behalf of the Trust, unless appropriately authorised to do so
  - employs false identity
  - creates, sends, forwards or replies to inappropriate material including, but not limited to, graphics, video clips, jokes, viruses and music files

- inappropriate use of email distribution lists (emails should be targeted to specific groups rather than to All Trust Staff. Trust Intranet Bulletin Boards should be used for general information relating to, e.g. surplus equipment)
- or uses that violate other Trust policies or guidelines
- the latter include, but are not limited to, policies and guidelines regarding sexual or other forms of harassment.

5.28 No e-mails may be sent externally outside of the Trust through the use of the automatic forwarding facility unless authorised. Staff must not use their personal email for work purposes.

5.29 Do not send large attachments unless absolutely necessary. Where drives are shared, indicate the location of the document in the e-mail so that the recipient can find the document. If you do send attachments you need to consider whether the document needs a copyright statement.

## 6.0 HOUSE KEEPING FOR E-MAIL SYSTEMS

6.1 Each mailbox has a storage limit and you must delete e-mail messages on a regular basis. If an important e-mail needs to be kept for future reference, save it in a personal folder.

6.2 If a Freedom of Information or Data Protection request is made all e- mails within your e-mail account could be shared if they are relevant to the request. Therefore ensure you delete your emails as soon as they are no longer needed ensuring that records management retention and destruction guidance is considered.

6.3 All email records destined for the internet will have an email disclaimer appended to the end of the email by the Trust systems. An example below details reference to the Freedom of Information Act 2000:-

*"The information contained in this email may be subject to public disclosure under the Freedom of Information Act 2000. Unless the information is legally exempt from disclosure, the confidentiality of this email, and your reply, cannot be guaranteed."*

## 7.0 SECURITY OF E-MAIL

7.1 When using the e-mail system, staff must be particularly aware of the following:

- vulnerability to unauthorised interception or modification;
- vulnerability to incorrect addressing;
- vulnerability to possible virus attachments;

7.2 Consideration should also be given to:

- the requirement to exclude sensitive information from the system;
- the exclusion of third parties from e-mail services.
- the use of NHS approved encryption techniques as they become available.

7.3 All staff will therefore comply with the following:

- treat e-mail as they would any other piece of correspondence, including appropriate language
- if the e-mail is regarding a patient/resident or staff member it should be printed off and filed in the person's record and then electronically deleted
- if an e-mail needs to be kept for other purposes, e.g. audit, it should be filed in the department's electronic system

## 8.0 CONTINUITY OF E-MAIL ACCOUNTS

8.1 When staff are going on planned leave/absence from the workplace they should ensure that the 'Out of Office' tool is implemented to ensure e-mail communications are not disrupted and that any urgent communications can be redirected where necessary.

8.2 Some staff will, due to the nature of their roles, need to set up 'authorised' deputies to access e-mails on their behalf during periods of absence.

8.3 Deputies should not be provided with log on or user passwords for their colleagues but use the appropriate process for e-mails to be collected via their own log on credentials.

8.4 Where staff are absent due to unexpected leave requirement instructions should be provided using a Network Change Control form by the person's line manager and forwarded to the ITT Service Desk who will arrange for deputy status for the appropriate colleagues to be established.

8.5 When a member of staff is away from the office for an extended period, for example holiday/sick leave or after leaving the Trust, there may be occasions when it is necessary to access email messages from their account without express consent. The reasons for this access could be;

- Subject access request under the Data Protection Act/General Data Protection Regulation (GDPR)
- Business Continuity (i.e. long term leave or illness)
- Freedom of Information request
- Evidence in legal proceedings
- Evidence in a criminal investigation
- Line of business enquiry
- Evidence in support of disciplinary action

8.6 Access to a staff member's mailbox without expressed consent can only be authorised by a Director or the Head of IT&T.

## 9.0 USING INTERNET/INTRANET SYSTEMS

***Acceptable Use:-***

9.1 The internet/intranet is to be used for work related purposes, for example to help with research for work, to access useful work related sites, for professional development and training or to obtain information related to work.

9.2 Any internet/intranet account provided by the Trust, assigned by the Trust to individuals, sub-units, or functions of the Trust, is the property of Essex Partnership University NHS Foundation Trust ('The Trust').

9.3 Those that use Trust internet/intranet services are expected to do so responsibly, that is, to comply with national laws, with this and other policies and procedures of the Trust, and with normal standards of professional and personal courtesy and conduct.

9.4 Access to Trust internet/intranet services, when provided, is a privilege that may be wholly or partly restricted by the Trust without prior notice when there is Substantiated Reason to believe that violations of law or policy have taken place, or, in exceptional cases, when required to meet time-dependant, critical operational need.

9.5 Access to internet/intranet will be inspected and/or monitored by Trust systems to protect the Trust, Trust Computing Facilities and account holders from internet/intranet borne viruses/macros/inappropriate attachments and/or content where possible.

9.6 The Trust shall permit the inspection, monitoring, or disclosure of internet access without the consent of the account holder of such sites which contain obscene, indecent, racist or illegal content:

- when required by and consistent with law
- when there is Substantiated Reason to believe that violations of law or of Trust Policies have taken place
- when there are Compelling Circumstances
- under time-dependent, critical operational circumstances as defined in the procedural guidelines (3.0).

9.7 It is understood that staff sometimes need to deal with personal / private matters during the working day. Limited personal use is therefore allowed provided it is kept to a reasonable level and does not interfere with the working day. This arrangement will be based on trust and all staff will be expected to use this facility in an appropriate manner. Staff should be aware that personal use of the internet will be monitored.

***Unacceptable Use:-***

9.8 Staff are reminded that they are bound by confidentiality clauses in their contract of employment and should take extreme care about the content of information they share if using social networking sites. Reference to

contact with friends or other members of the public in the course of their work should be avoided to prevent potential breaches of confidentiality.

9.9 Access to the internet/intranet is provided for staff to use in the course of their work. Staff are prohibited to access, view, download, display or distribute any of the following:

- Content that expresses personal views about subjects unrelated to and inappropriate for a productive workplace;
- Accessing sites that relate to or provide information on criminal or terrorist activity; and/or
- Accessing sites that the whole prime function is to provide offensive materials. Posting, downloading or viewing pornography may constitute a criminal offence and is likely to be viewed as gross misconduct warranting summary dismissal.
- Anything which is otherwise offensive

9.10 Where staff inadvertently access websites which may fall into the group above (9.9) this should be reported to the Trust's ITT Helpdesk immediately.

9.11 Trust internet/intranet services may not be used for:

- unlawful activities
- commercial purposes not under the auspices of the Trust
- personal use that:
  - directly or indirectly interferes with the Trust operation of computing facilities, internet or email services
  - burdens the Trust with noticeable incremental cost
  - interferes with the user's employment or other obligations to the Trust
  - gives the impression that the user is representing, giving opinions, or otherwise making statements on behalf of the Trust, unless appropriately authorised to do so.
  - employs false identity
- or uses that violate other Trust policies or guidelines
- the latter include, but are not limited to, policies and guidelines regarding sexual or other forms of harassment.

9.12 Staff must not use the internet, to attempt any unauthorised access to resources (hacking). Nor are staff allowed to access hacker websites as some sites contain traps which may trigger malicious programmes when a page is read.

***Joining Chat Rooms and News Groups:-***

9.13 Staff may join a chat group or news group related to work. Staff are required to conduct themselves in a professional manner, be courteous and inoffensive. Unless you are authorised to do so, staff are not permitted to write or present views on behalf of the Trust or any NHS organisation. Some groups may require permission to be granted for access. Under no circumstances should patients be identified during discussions.

(*Refer to the Social Media Policy/Procedure for further guidance.*)

## 10.0 OBTAINING E-MAIL ACCESS

10.1 Where an e-mail account has not been provided to an individual at the stage when their network account has been set up, the line manager must make a request to the relevant ICT service provider using the appropriate approval route.

10.2 The IT&T Department will install software to enable staff to access the Trust e-mail facilities. The software must not be reconfigured by members of staff, other than those in the IT&T Department.

10.3 Only software provided by the Trust's IT&T Department may be used to access e-mail facilities.

## 11.0 MONITORING INTERNET/INTRANET/E-MAIL SYSTEMS

11.1 A username and password restrict the use of internet/intranet/e-mail services. All use of the system is logged against the username and the Trust will assume that this is the authorised person accessing the facilities.

11.2 Trust staff must not share usernames or passwords with colleagues.

11.3 In the event of abuse/misuse of the Trust's internet/intranet/e-mail services all access will immediately be revoked pending any investigations and staff may be investigated through the Trust's disciplinary procedures in the event that abuse of internet/intranet/e-mail services is proven.

11.4 The automated monitoring software used provides an audit trail of the addressee, recipient and contents of the e-mail. We reserve the right to monitor your use of e-mail at any time for operational reasons and to review, monitor, replicate, audit and disclose any material held on any IT system, including laptops owned by the organisation, to investigate and guard against the misuse of e-mail. If a breach of e-mail use is detected, a full enquiry will be undertaken. Disciplinary procedures may be started which may ultimately lead to dismissal or criminal prosecution. Serious offences, even for the first time, may constitute gross misconduct justifying summary dismissal.

11.5 The automated monitoring software used provides an audit trail of who logged on to an internet site, when, for how long, which sites were accessed, number of attempts to access sites and whether a file transfer took place. Offensive site access is tracked and excessive use of the internet is flagged up. Staff need to bear in mind that some sites track the unique address for your computer (IP-address) so they can track you or the organisation you work for. We reserve the right to monitor your use of the internet/intranet at any time for operational reasons and to review, monitor, replicate, audit and disclose any material held on any IT system, including laptops owned by the organisation, to investigate and guard against the

misuse of internet/intranet access. If a breach of internet/intranet access is detected, a full enquiry will be undertaken. Disciplinary procedures may be started which may ultimately lead to dismissal or criminal prosecution. Serious offences, even for the first time, may constitute gross misconduct justifying summary dismissal.

**END**