Bolton NHS
NHS Foundation Trust

Email and Internet Usage Policy

Document type:	Policy
Version:	4.2
Author (name):	Ken Bradshaw
Author (designation):	Informatics Programme Manager
Validated by	E-Communications Group
Date validated	14th September 2015
Ratified by:	IT and Information Committee
Date ratified:	6th November 2015
Name of responsible committee/individual:	E-Communications Group
Name of Executive Lead (for policies only)	Andy Ennis Director of Operations
Master Document Controller:	Rebecca Moden
Date uploaded to intranet:	20th November 2015
Key words	Web www, security, data, email ,informatics
Review date:	6th November 2017

Version control

Version	Type of Change	Date	Revisions from previous issues
V4.1	Minor Review	August 2015	Minor changes to reflect new template requirements and to incorporate reference to Social Media Policy
V4.2	Minor review	October 2015	Correction of minor typographical errors and removal of paragraph 43

Equality Impact

Bolton NHS Foundation Trust strives to ensure equality of opportunity for all service users, local people and the workforce. As an employer and a provider of healthcare Bolton NHS FT aims to ensure that none are placed at a disadvantage as a result of its policies and procedures. This document has therefore been equality impact assessed to ensure fairness and consistency for all those covered by it regardless of their individuality. The results are shown in the Equality Impact Assessment (EIA).

Contents

Purpose of the Email and Internet Usage Policy

1. The Email and Internet Usage Policy provides guidance about acceptable use of Email and Internet using hardware, software and networks provided by Bolton NHS Foundation Trust. The Policy also describes the standards that users are expected to observe when using these facilities and ensures that users are aware of the legal consequences attached to the inappropriate use of the facilities.

2. The policy also aims to ensure the security of Bolton NHS Foundation Trust IT assets in order to:

   - ***Ensure Availability***: that is to ensure Trust IT assets are available when required to support the Trust’s business and objectives

   - ***Preserve Integrity:*** that is to protect the Trust IT assets from unauthorised or accidental modification to the accuracy and completeness of the Organisation’s assets.

   - ***Preserve Confidentiality:*** that is to protect information from unauthorised access and disclosure.

   - ***Ensure Legality:*** that is to ensure that the Trust and its employees comply with legislation and NHS policy and standards

3. This policy should be read in conjunction with the Social Media Policy

Introduction

4. Bolton NHS Foundation Trust recognises that the Internet and Email are valuable resources and wishes to encourage use of these facilities to develop the skills and knowledge of its workforce to benefit its corporate and professional objectives.

5. However, the nature of the Internet and Email raise concerns about security, confidentiality and proper conduct. This policy seeks to clarify these issues and avoid ambiguity, so as to protect the Trust and its staff.

6. This policy is not a definitive statement of the purposes for which the Trust’s facilities must not be used. The onus is placed upon the user of the Trust’s systems to conduct themselves at all times in a trustworthy and appropriate manner so as not to discredit or harm the Trust, its patients or its staff.

7. The provision of Internet access and Email relates primarily to use for the Trust’s business. Limited personal use is also permitted provided this does not interfere with the work of the user, their colleagues or the interests of the Trust.

8. The Trust uses automated mechanisms, both passive (e.g. logging) and active (e.g. blocking access to certain categories of web site), to ensure compliance with this policy. Where the Trust has reason to believe that inappropriate use of the Email or Internet facilities is or has been occurring an investigation will be undertaken in line with the Information Security Policy and disciplinary procedures.

9. This document is intended to cover Email and Internet access from both within the Trust and remotely from any other location. All usage of the Trust's Email or Internet resources will be governed by the guidance detailed within this document.

10. Staff are reminded that only those staff who are specifically authorised to give media statements on behalf of the Trust, only the Trust Communications Manager, may write or present views, concerning the Trust and its business.

Legal implications

11. Email has become established as a means of personal communications and its use is now widespread. Several factors combine to make Email a particularly important issue where Data Protection, Freedom of Information and the management of personal information is concerned.

12. Misuse of Email can result in legal liability for the Trust and, in some cases, the individual user and their managers. Inappropriate use could, for example, give rise to liability for defamation, copyright infringement, breach of confidentiality, negligent virus transmission, inadvertently entering into contracts, harassment and discrimination, in addition to breaches of the data protection legislation.

13. Email and the Internet are considered a form of publication and therefore inappropriate use of the Internet or Email may constitute a libel contrary to the provisions of the Defamation Act (1996).

Scope

14. This policy applies to all members of staff employed by Bolton NHS Foundation Trust. It also applies to honorary contract holders, seconded staff, locum staff, bank staff, voluntary workers and agency staff using the resources of the Trust, as well as contractors and any others working on behalf of Bolton NHS Foundation Trust or staff from other trusts using the Trust's facilities.

15. All members of staff and those identified above are required to adhere to this policy. Managers at all levels are responsible for ensuring that their staff are aware of and adhere to this policy.

16. The Policy refers to all user activity in relation to Email, NHSnet and the Internet using computers (including laptops, and other mobile devices) based on all Trust sites or used via the Trust's network

The Organisation's Responsibilities

17. The Trust will take all reasonable steps to ensure that users of the Internet service are aware of policies, protocols, procedures and legal obligations relating to the use of Email and the Internet. This will be done through training and staff communications at departmental and organisation-wide levels.

18. The Organisation will ensure all users of the Email and Internet facilities are registered and that access is linked to agreed levels of authority.

19. Under no circumstances will patients and visitors be given access to Trust data and systems including access to Internet and Email facilities using Trust equipment please refer to the Social Media Policy for further guidance.

Operational Responsibilities

Staff

20. Must adhere and abide by the Email and Internet Usage Policy.

21. Should have an understanding of the responsibilities and risks associated with the use of Email and Internet.

Managers

22. Are responsible for the identification of staff training requirements and for making arrangements for addressing staff training requirements through individual personal development plans.

23. Are responsible for ensuring that their staff are aware of the Email and Internet Usage Policy guidance, its requirements and implementation.

24. Should review the usage of the Internet access made by their staff, , to ensure that staff access to the Internet facilities does not interfere with Trust business. Where managers have concerns about staff internet use they can request usage reports via the IT Service Desk.

25. Where staff have concerns about the records relating to their own access they can request usage reports via the IT Service Desk.

Internet Access – General Principles

26. Staff who do not use a computer for their work may have access to a designated computer in their department or location at the discretion of their line manager. Staff may use the facilities in the Post Graduate Medical Centre Library.

27. Staff must not access or distribute any material which is (or participate in any chatroom or Internet community whose subject matter is) unlawful, or causing of offence, examples of which are material which is libellous or pornographic or which includes offensive material relating to gender, race, sexual orientation, religious or political convictions, or disability. This also includes incitement of hatred and violence or any activity that contravenes the Trust's Policies including Equal Opportunities Policy. This requirement applies even if a specific site is not blocked by the Trust access control software.

28. Access to Internet sites will be controlled by content management software which blocks access to sites considered inappropriate.

29. Access to categories of sites that are not considered to be business related will be permitted, but this is not an entitlement and should not impact normal daily work. Managers will be actively monitoring usage and will take appropriate action in the event of excessive use. In particular, access to social media sites (such as Facebook) will be blocked but access to professional networks (such as Linkedin) will not. Users can request access to social network sites for stated business purposes for a specified period of time, with their line manager's approval, through the IT Service Desk. Further guidance is set out in the Social Media Policy.

30. If an employee accidentally accesses material which they feel may be considered of an offensive nature, they may wish to note the time and web site address, exit from the site and then inform their line manager.

31. If an employee is in doubt about whether it is appropriate for them to access a site, they should obtain the approval of their line manager before doing so.

32. Internet users must be aware that the Internet is inherently insecure and confidential information in relation to the business of the Trust and/or person-identifiable information must never be disclosed.

33. Although the Trust has anti-virus defences in place, great care should be taken when using the Internet. The IT Service Desk (ext. 5950) should be informed if any suspicion of virus infection arises.

34. Downloading or distribution of copyrighted material without permission of the copyright holder, or of software for which the user does not have a legitimate licence is forbidden, this applies equally to downloads for work or personal use.

35. Access to sites or services providing file sharing services or file storage facilities is forbidden except where provided by the Informatics Department.

36. Access to media streaming sites, such as will be blocked unless it is required for business purposes. Streaming media uses significant network bandwidth and can affect the performance of business applications, including clinical systems. Users can request access to media streaming sites for stated business purposes for a specified period of time, with their line manager's approval, through the IT Service Desk.

37. Access to cloud storage sites, such as Dropbox and SkyDrive will be blocked to prevent data loss.

Use of Email – General Principles

38. Any Email sent or received by an employee is deemed to be Trust property and as such is subject to the Trust's Records Management policies and procedures. Unless marked Personal in the 'Subject Field' Email may be opened by the Trust. It must be noted, however, that any Email marked 'Personal' may be opened in such circumstances that include:

39. Access under the Regulation and Investigatory Powers Act which would require Chief Executive approval and would be used in circumstances where for example a crime was suspected.

40. As part of an automated process to allow encryption to take place i.e. non-human intervention

41. In response to a request under the Data Protection Act , Freedom of Information Act and potential Access to Health Records Act

42. In circumstances were the individual was on long term sick or unavailable and business continuity arrangements required access - this would be approved by a line manager for access by a nominated individual.

43. Distribution Lists will be created on request by the Informatics Department. A nominated Email mailing list will be created on request by the IT Department by default all staff will be added to the list but can remove themselves via the Intranet AD Self-Service option.

44. When using the Email service for personal correspondence, the amount and time that an employee may use the Email system for reasonable personal access should be agreed with their line manager.

45. Staff must not distribute any material which is unlawful, or causing of offence, examples of which are material which is libellous or pornographic or which includes offensive material relating to gender, race, sexual orientation, religious or political convictions, or disability. This also includes incitement to commit a crime, incitement of hatred and violence or any activity that contravenes any of the Trust's policies including Equal Opportunities Policy. This also includes material that could be classed as abusive, indecent, obscene, menacing; or in breach of confidence, copyright, privacy or any other rights. Distribution of such material may result in legal action in addition to Trust disciplinary procedures. The Trust reserves the right to monitor all Email and is required to do so under law according to Principle 7 of the Data Protection Act (1998).

46. Staff must not initiate or forward electronic chain letters, forge or anonymously send Email or make any attempt to infect other systems with computer viruses. If staff receive such Email and have concerns over the content, they should contact the IT Service Desk (ext 5950).

47. Staff who receive Email attachments which they have any doubts about the origin and/or content of should contact the IT Service Desk for advice.

48. Under no circumstances is patient identifiable data or sensitive information to be sent over the Internet in an unencrypted form.

49. Where any Email which is to go outside of the Trust and it contains person identifiable data or sensitive information the user must set the sensitivity option for the Email as Confidential and software deployed by the Trust will encrypt the Email.

50. Under no circumstances should web mail services such as, Hotmail and Googlemail be used for Trust related activities. Access to web mail services where possible will be blocked with the exception of doctors.net.uk.

51. Guidance on Email etiquette is given in Appendix 2.

Email Retention

52. Decisions on which records to retain and for how long are dictated by legislation, internal regulations and their value to the Bolton NHS Foundation Trust.

53. Email records will be subject to records appraisal using administrative, legal, fiscal and archival guidelines to establish the value of the record. The value of the record will be determined on the informational content of the Email not on the medium on which it resides.

54. The Bolton NHS Foundation Trust has in place retention schedules which dictate the periods for which records should be retained and later destroyed. These retention schedules are part of the records management system and should be used to determine the records lifecycle. Specialist retention schedules may be used at a departmental level where a greater level of detail is required.

55. If a user wishes to archive Emails the advice of the IT Service Desk should be sought.

Monitoring of Email and Internet Activity

56. Bolton NHS Foundation Trust will maintain monitoring arrangements in relation to all Internet, Email and related services and facilities that it provides and will apply these monitoring arrangements to all users.

Internet access

57. Access to the Internet is logged on a per user basis; details such as the date and time of access, and the site visited are recorded. Reports using this information can be provided to a user's line manager or superior.

Email Activity

58. The Trust currently retains a copy of all Email which is sent within and outside of the Trust and is received by the Trust. The Trust will not use this facility to monitor employees' Email traffic without cause.

59. The Trust will typically investigate inappropriate activity under the following circumstances:

    - a report by a member of staff to their line manager raising concern about the contents of a computer or of an Email

    - A concern is raised by a line manager about inappropriate personal use of a Trust computer

    - Routine monitoring identifies potential inappropriate use

    This list is not exhaustive

60. The Trust may, at its discretion, apply automatic message monitoring, filtering and rejection systems as appropriate, and deny transmission of messages with content that is unacceptable in the terms of this Policy. Files with specific extensions will be automatically blocked e.g. EXE,DBF.

61. The Trust reserves the right to carry out detailed inspection of any IT equipment without notice, where inappropriate activity is suspected. More detailed investigation could involve further monitoring and examination of stored data (including employee deleted data) held on servers, disks, drives or other historical/archived material

62. IT support staff will be responsible for username and password management, virus control and the management of security and the Internet connections. Users should not share their password and not leave their computers unattended whilst logged on, as they will be held responsible for any activity, which takes place using their account. Unauthorised use of someone else's identity to access the Internet or send Email is strictly forbidden and will result in disciplinary action.

63. All users need to be aware that the Email service is within the ownership of the Trust and therefore the Trust can access any mailbox if there is a valid reason for doing so.

64. Other than for the monitoring purposes already referred to, access to the content of any staff member's mailbox in their absence will only be granted on submission of a written request from their line manager, the Freedom of Information Office or from the Trust's Counter Fraud Specialist under the NHS Counter Fraud Strategy, to the Chief Informatics

Officer or a designated deputy. This request must identify the business need for the access requested and indicate the Email message/s to be examined.

65. In the event that a user will be absent for an extended period of time, then access to their entire mailbox may be granted to their line manager.

66. It is accepted that a limited amount of personal messages will be sent using the Trust's Email system. These messages must be marked as 'Personal' in the 'Subject' field of the Email. Any Emails not marked with the required text may be opened and the contents viewed as described above.

67. Under the Freedom of Information Act (2000), any Email unless marked as personal may be accessed under the provisions detailed in the legislation.

Training and Awareness

68. The Informatics Department will undertake training on the use of the Internet and Email facilities where requested, and will raise awareness of this policy and related issues through staff induction, staff handbooks and Emails to staff. This policy is also available from the policy area on the Trust Intranet.

Monitoring Compliance

69. Compliance with this policy will be monitored as set out below

Area to be monitored	**Methodology**	**Who**	**Reported to**	**Frequency**
Internet Usage	Compliance Report	IT Department	E-Communications Group	Quarterly
Internet Usage	Ad Hoc Reporting	IT Department	Departmental Managers	On Request
Email Usage	Ad Hoc Reporting	IT Department	E-Communications Group	Ad Hoc

Appendix 1 Email Etiquette and Good Practice

Junk Mail

Email should not be sent to large numbers of people unless the sender is sure that it is directly relevant to that job. Sending unsolicited mail to many users (‘spamming’) is wasteful of user time and can disrupt the service for others.

Note: Items of general Trust-wide interest (e.g. ‘wanted items’) should, unless there are good reasons to the contrary, be posted on the Trust’s intranet and should not be published to ‘All Internal Users’ on Email

Large Files

Sending of very large files (>10Mb-bidirectional) should be avoided where possible. Should users wish to send such files on a regular basis, they should contact the IT Service Desk to make appropriate arrangements.

Housekeeping

Users are allocated a specific resource for storing Email. When the size of the maximum limit has been reached they should ensure that the relevant items are archived, deleted or moved to a desktop folder. If there is an Email that may be required in future it should be archived. The sharing of calendars and mailboxes are set by the user and responsibility will rest with the user for their correct application

Mailbox Owners

Email users should review their Email at regular intervals (at least twice daily). When unavailable, users should divert their mail to an authorised person or notify others of your inability to read your mail by using the mailbox tools available.

Address Books

Users must take care when selecting recipients from the Email address books, as they may inadvertently select the wrong person or group of people and send sensitive information to them. Be selective about who receives your Emails, especially when using “Reply to All”. Do all recipients need to see the reply? Use organisation wide distribution lists only to communicate important business information that has genuine site wide value.

Accuracy

Always check the Email before dispatch for spelling and grammar.

Email Etiquette

When you are sending messages or responding to messages sent by other users, your recipient might have different views, opinions and cultures. Without vocal inflection and body language sarcasm, facetiousness and otherwise innocent ‘fun’ can easily be misinterpreted as being rude or abusive.

Email messages should NOT be written in all CAPITAL letters as this is considered to be aggressive.
The Subject field should always be used to add a short description of the contents of the Email. This will assist the recipient in prioritizing opening of Email and aids future retrieval of opened messages.

Care should be taken with content. Nothing should be written in an Email that would not be written in a letter or said to someone face to face.

The same conventions should be used as when sending a letter by post, e.g. using the same style of greeting.

Emails should be signed off with the name, title and contact details of the sender. This can be added to a signature file so that it appears automatically by selecting File – Options – Mail – Signatures.

Example Signature:

Tracey Moss
PA to Simon Worthington, Finance Director
Bolton NHS Foundation Trust | Trust HQ | 1st Floor | Royal Bolton Hospital | Minerva Road | Farnworth | Bolton | BL4 0JR |
Tel: (01204) 390684 (internal ext. 5684)| Email: tracey.moss@boltonft.nhs.uk | Working days: Monday to Thursday
Website: www.boltonft.nhs.uk | Follow us on Twitter: @boltonnhsft

Appendix 2 Equality Impact Assessment Tool

To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

		Yes/No	Comments
1.	**Does the document/guidance affect one group less or more favourably than another on the basis of:**		
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender (including gender reassignment)	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation	No	
	• Age	No	
	• Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are there any valid exceptions, legal and/or justifiable?**	No	
4.	**Is the impact of the document/guidance likely to be negative?**	No	
5.	**If so, can the impact be avoided?**	No	
6.	**What alternative is there to achieving the document/guidance without the impact?**	N/A	
7.	**Can we reduce the impact by taking different action?**	N/A	