Bolton NHS
NHS Foundation Trust

Information Security Policy

Document type:	Policy
Version:	5.1
Author (name):	Ken Bradshaw
Author (designation):	Joint Chief Informatics Officer
Validated by	IG Group
Date validated	16th March 2016
Ratified by:	IT and Information Committee
Date ratified:	24th March 2016
Name of responsible committee/individual:	IG Group
Name of Executive Lead (for policies only)	Andy Ennis Director of Operations
Master Document Controller:	Rebecca Moden
Date uploaded to intranet:	24th March 2016
Key words	IT, Data, Information, Virus, Access, Communication, Mobile, Remote, Password
Review date:	26th February 2018

Version control

Version	Type of Change	Date	Revisions from previous issues
V5.1		February 2016	Major reformatting Changes to reflect user authentication processes Addition of requirements relating to two factor authentication Added EM-1 Form

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

Information Security Policy

The need for an Information Security Policy

1. This policy has been developed to protect the Trust, its staff and patients, from issues related to the storage and exchange of confidential information using information technology. The aim is to protect the Trust from accidental or deliberate unauthorised access or disclosure of information. The policy applies to all business functions and information contained on the network or devices owned or used in conjunction with Trust business.
2. This policy is based upon the ISO27001 standard - a code of practice for information Security Management.
3. Key issues addressed by this security policy are:

   Confidentiality - Information is confined to those with specific, explicit authority to review the information.

   Integrity - Safeguarding the accuracy and completeness of information.

   Availability - Ensuring authorised users have access to information when required.

4. This policy seeks to protect the information held by Bolton NHS Foundation Trust and to minimise opportunities for its misuse and loss. Both are critical to statutory compliance and the delivery of patient care.
5. The Trust's Information Security Policy will be developed and updated on a continuous basis informed by regular risk assessment and review.
6. This policy applies to everyone who has access to Bolton NHS Foundation Trust' Computer Information systems and manual records.

Scope of Information Security Policy

The Trust's policy aims to ensure that:

- Information and information systems are properly assessed for security.
- Confidentiality, integrity and availability are maintained.
- Staff are aware of their responsibilities, roles and accountability.
- Procedures to detect and resolve security breaches are in place.
- Information security issues are dealt with consistently throughout the Trust.

Managers' Responsibilities

- All managers share responsibility for information security.
- Ensure that staff are instructed in their information security responsibilities.
- Ensure that staff using information systems/media are trained in their use.
- Ensure that no unauthorised staff or third parties are allowed to access any of the Trust's Information systems.
- Determine which individuals are to be given access to specific information systems.
- Ensure that current documentation is always maintained for al critical job functions as part of business continuity planning, and to ensure continuity in the event of unavailability.

- Ensure that the IT Service Desk and other appropriate staff are advised about staff changes affecting information access (e.g. job functions, leaving etc).
- Ensure the physical security of all IT equipment used in their area of responsibility

Staff Responsibilities

7. All staff must:
   - Ensure that no unauthorised persons are allowed to access any of the Trust's Information Systems.
   - Not disclose password or details of information security arrangements except to authorised staff.
   - If systems do not enforce password change users must change passwords at regular intervals.
   - Co-operate in the implementation of this policy to minimise risk to the Trust.
   - Adhere to their professional codes of practice.
   - Report suspected breaches of the policy to their managers.
   - Must adhere and abide by the Email and Internet Usage Policy.
   - Should have an understanding of the responsibilities and risks associated with the use of Email and Internet.
   - Must read the policy and sign the Acceptance Document, located in Appendix A.

Password Rules

8. All staff must use a complex password for IT network access and for IT applications (where those applications allow) which consists of 3 of the 4 items listed below and
   - At least one upper case letter (A – Z)
   - At least one lower case letter (a – z)
   - At least one number (0 – 9)
   - At least one special character (!£$%^&*)
   - Complex passwords can be easily remembered by applying the rule to a phrase i.e. mycarcost£300 Cat&2dogs
9. Where systems allow, users should be prompted to change passwords every 90 days.
10. Remote connections by staff will require two factor authentication using an appropriate solution provided by the Trust

Specialist Advice

11. Specialist advice on Information Technology Systems and security arrangements shall be provided by the IT Service Desk. Advice on legal or compliance issues shall be provided by the information Governance Manager. General security advice shall be provided by the Trust's Security Manager.

Risk Management

12. All Trust Information systems shall be subject to periodic security reviews by the respective System Managers. Security will be reviewed in accordance with the Trust's Risk Management policy and procedures.
13. Individual systems shall be reviewed at least once every 3 years.

14. The Trust shall ensure that Business Continuity Plan are in place and up to date for all Information systems as determined by risk assessment.

Security - Third Party Access

15. Access to Trust's information by third parties will be strictly controlled.
16. Where access by a third party is required, a risk assessment shall be conducted and control requirements identified and agreed. These shall be identified in any associated contract.
17. Where remote hosting is proposed attention shall be given to ensuring that the information security arrangements offered by the proposed supplier are as at least robust as those in place within the Trust.

Transfers of Personal Identifiable Information

18. All patient identifiable data to be transferred on electronic media to recipients outside the Trust must be encrypted
19. All new bulk transfers of personal identifiable information (20 patients or more), whether on paper or on electronic media (including but not restricted to CDs, DVDs, USB mass storage devices, floppy disks) must be registered with and approved by the Information Governance Manager.
20. Where patient identifiable data has to be sent by registered post/courier unencrypted, including images, there must be no alternative means of sending the data. It must be justified on the basis that by not sending this data it would prejudice patient care.

Equipment Security

21. All central processors/networked file servers/network equipment shall be located in secure areas with restricted access.
22. Local network equipment and network terminating equipment shall be located in secure areas/and or lockable cabinets.
23. Equipment shall be protected from power supply failure where appropriate.
24. All equipment including PCs and laptops must be located in secure areas and/or secured to protect from theft.

Equipment Procurement

25. All information processing and storage equipment shall be procured in accordance with the Information Technology Procurement Policy.
26. All procurements will conform to Trust's standing financial instructions and must have the approval of the Informatics Department.

Communication Routing

27. All communications cabling between buildings shall be via underground conduit not accessible to unauthorised persons.
28. All communications cabling within buildings shall be in conduit if surface mounted, otherwise in the framework of the building.

Equipment Maintenance

29. All information processing equipment shall be covered by maintenance agreements, with appropriate response levels as indicated by risk assessment.
30. All third parties supplying such services shall be required to sign confidentiality agreements.

Remote Diagnostic Services

31. All suppliers requiring remote access shall commit to maintaining confidentiality of data and information using only qualified personnel.

32. Requests for remote access shall be authorised by the IT Service Desk. Strong authentication is the preferred method. All suppliers who connect via the NHS N3 network must have signed a Code of Connection agreement

Remote Connections and data transfers

33. Definitions

- **Mobile data devices** – this includes any device that can store information required for the organisation's operational business. Typically this is laptops, tablets,smart phones and other mobile devices but also includes digital audio and visual recording/playback devices (such as Dictaphones and digital cameras).
- **Media** – Any physical item that can store information and requires another device to access it. For example, CD, DVD, Floppy disc, tape, digital storage device (flash memory cards, USB disc keys, portable hard drives)

Data and Information Transfers

34. The authorisation procedure only relates to staff that need to use mobile computing facilities, either on or off-site (including staff homes), or transfer information between computer systems via physical media. Staff making offsite usage of paper will be subject to the overall 'Information Security Policy'. Specific procedures around authorising the access, use and tracking of medical records detailed within medical record policies are not replaced by this document.

35. Users of information will:

- Keep usage to a minimum in public areas
- Only use information off-site/at home for work related purposes
- Ensure security of information within the home
- Not permanently store patient or staff identifiable data on equipment not supplied by the organisation
- Scan any media used to transfer data for viruses when accessing it via organisational equipment
- Not send patient or staff identifiable data to home (internet) email addresses without encryption. See also section 7.
- Keep equipment and files locked out of sight during transit
- Ensure equipment and files are adequately packaged in transit to prevent damage or tampering
- Not dispose of any media (including paper) off-site
- Will not leave any equipment unattended without adequate additional security measures (such as cables and locking it away)

Physical Security/Access control in any public access area

36. The use of information in these areas will be kept to an absolute minimum, due to the threats of 'overlooking' and theft. Any member of staff choosing to use information and/or devices in these areas that results in any related incident will be required to

state why the usage was required in that situation and the efforts they made to protect the information and any equipment.

37. Mobile or portable equipment in use should not be left unattended at any time. (NB for controls on transportation of equipment see section 8)

Physical Security / Access control in in areas not generally accessible to the public (including. other organisational premises)

38. Staff are responsible for ensuring that unauthorised staff are not able to see information or access systems. If equipment is being used outside of its normal location and might be left unattended, the user will secure it by other means (such as security cable).

Physical Security/Access control for Occasional usage at home

39. Only members of staff are allowed access to information being used at home in any form, on any media.
40. Use of any information at home must be for work purposes only
41. Staff must ensure the security of information within their home. Where possible it should be stored in a locked container (filing cabinet, lockable briefcase). If this is not possible, when not in use it should be neatly filed and stored in a way that it is not obvious to other members of the household.
42. Any personal/sensitive (inc. patient and staff information) or organisationally confidential information that has to be taken home, must be within folders marked 'private and confidential' and other members of the household instructed not to look at it.

Physical Security/Access of Supplied equipment

43. Where the organisation has supplied any form of data device only the member of staff themselves is authorised to have any access to it.
44. Any member of staff allowing access to an unauthorised person, deliberately or inadvertently will be subject to the organisations disciplinary proceedings.
45. You may not connect any supplied equipment to any phone line or internet connection or other computer, other than where you have been given authority and access to either the NHS N3 network or your / organisation's network via a secure remote link.
46. Any equipment supplied for remote access to NHS N3 network or the organisation must be stored securely when not in use. Where a system requires a PIN number and a 'security token' these must be stored separately
47. The Informatics department is responsible for ensuring that access to supplied equipment requires a username and password and that anti-virus software is installed.
48. For supplied equipment that is not classed as portable (i.e. a supplied desktop PC), the Informatics department is responsible for ensuring anti-virus software is regularly updated.
49. If you have been supplied with portable equipment (i.e. a laptop or similar device), you are responsible for ensuring that it is regularly connected (maximum of 3 months) to the organisation's network 'on-site' for upgrade of anti-virus software .
50. Person Identifiable Data files should have additional protection against unauthorised access using file permissions. Contact the Informatics Help Desk if you do not know how to do this.

51. When equipment is returned or the data is no longer needed the data should be removed. Contact the Informatics helpdesk if you do not know how to do this.
52. Provided all policy statements above are applied, you may use any supplied equipment for any type of work you would normally do on an organisational desktop PC, including the use of confidential information provided you comply with general regulations on handling and storing confidential data.

Physical Security/Access of Staff owned equipment

53. The storage on hard disk or portable media of Patient and Staff Identifiable data (or data on any individual) or other sensitive date (such as commercial or legal data) on staff owned equipment is strictly forbidden.
54. Organisation information (such as spreadsheets, plans, reports etc) may be used, but must not be permanently stored on the equipment. Please note any document transferred via email is stored on the receiving PC until specifically deleted.
55. To restrict the possibility of viruses being transmitted to the organisation's computers and network, staff must not use their own computer for work related activities unless anti-virus scanning software has been installed.
56. When you transfer files from your personal home computer to the office environment via floppy disk (or other removable media) you must virus scan them when loading them onto your office computer using the virus scanning software. Contact the IT Service Desk for information on how to do this if unsure.

Physical Security/Access relating to Teleworking

57. Teleworking is defined as a member of staff who regularly spends large parts of the working day, working from their home location. It does not refer to staff who spend the occasional afternoon working from home, or take work home in evenings 'to finish something off'. The decision as to whether a member of staff is a 'teleworker' will be taken by their line manager, based on the frequency of work being done from home and the equipment required to support it.
58. Sensitive information (person identifiable or organisationally sensitive) must be locked away when not in use and only accessible by the member of staff.
59. Any controlled document (e.g. patient record) they have will be traceable to their location and that any procedure to note the location of a file required by the organisation will be rigidly applied by them.
60. They should adopt procedures to 'back up' data files on computer Authorisation to Remove Data Files
61. All staff who need to work with Person Identifiable or Organisationally Sensitive Data should have authorisation from your line manager before data files can be taken off-site. Where approval is given and where it is deemed necessary to store information the following conditions apply:
62. Devices must be owned and maintained by Bolton NHS Foundation Trust
63. Password authentication must be applied all information must be encrypted
64. Its shall be stored only for the time when it is actually being used and deleted after use
65. Only the minimum amount of personally identifiable information needed for the current purpose shall be stored
66. The physical security of the device must be actively considered

67. The manager must keep a record of all persons authorised to remove data or approved to work remotely.

Sending Confidential Email to and from Home

68. The organisation has an e-mail policy to refer to but the following points apply directly to staff working from home.

Patient Identifiable Data Contained in an email

69. Patient identifiable data must not be sent to a personal email address without additional security such as 'encryption'. Internet e-mail services of any sort are not secure and should not be used to send Person Identifiable or other confidential information.

Auto forwarding of email

70. Staff must not automatically forward their e-mail to a commercial ISP (Internet Service Provider) such as Hotmail to enable access at home. Staff sending e-mail should be aware that it is not suited for confidential communications. Various systems are used for receiving e-mail and there is no guarantee that the addressee will be the only person to see the mail.

Transport of Equipment, Files and Paper Documents

71. When you remove equipment, files and data from organisational premises you are responsible for ensuring its safe transport as far as is reasonably practical.
72. Equipment, and paper files should be kept out of sight (in car boots), locked away and ideally not be left unattended at any time. Do not leave in cars overnight
73. IT equipment must be transported in a secure, clean environment. Equipment is not insured and you may be held liable if you do not take reasonable precautions.
74. Appropriate packaging (such as sealed envelopes, bubble wrap etc) will be used to prevent physical damage
75. Where a courier service is used to transport packages (potentially to teleworkers) containing sensitive information tamper proof packaging will be used. Courier firms should guarantee the safe arrival of parcels and the confidentiality of any contained information.
76. All data must be encrypted and the electronic transfer of information using secure network technology should be the preferred means of data transfer.

77. Disposal of media (electronic & paper)

78. All disposals of media will take place on-site of the organisation in line with on-site disposal procedures. No media will be disposed of at home. Staff with media to dispose of are responsible for returning it to site.

79. Disaster Recovery/Major incident planning

80. In the event of a major incident or disaster, the organisation may recall all equipment on loan to provide core services.

81. Termination of Employment

82. On leaving the employment of the organisation, all equipment, software and information must be returned.

83. Legal Liability

84. The organisation is legally empowered to report any criminal activity to the Police. Use of organisationally owned equipment to download, store and/or send offensive material is prohibited. In some cases criminal prosecution may be required.

85. Individuals must still adhere to Trust Policies of Internet and Email usage. Any defamatory material for example would be the responsibility of the individual

86. Disposal of Equipment and Media

87. All IT equipment, including all electronic devices which store data, shall only be disposed of in accordance with the WEEE (Waste Electronic and Electrical Equipment) regulations and must follow the Disposal of Redundant IT Equipment process. Requests to dispose of IT equipment must be made through the IT Service Desk.

88. All information shall be removed from IT equipment scheduled for disposal.

89. All removable digital media, including disks, USB memory sticks and flash drives must be securely reformatted or degaussed before disposal - if this is not possible the media must be physically destroyed.

90. All confidential or sensitive information held in non-digital forms (paper, film etc.) shall be shredded or burnt.

91. Security Incidents

92. A record of computer systems malfunctions will be maintained by the IT Service Desk together with a record of the remedial action taken.

93. Breaches of information security will be reported as quickly as possible using the Safeguard system, in accordance with the Trust's "Investigation and Reporting of Red Serious Untoward Incidents and Amber Divisional / Departmental incidents" policy.

94. Breaches of security confidentiality shall, as appropriate, be dealt with in accordance with the Trust's disciplinary procedures.

95. Regular analysis of malfunctions and breaches of security shall be undertaken as a security analysis aid and as a means of learning from incidents. Where appropriate lessons can be disseminated via the Governance and Information Governance Committees. Investigations of incidents will be carried out by appropriately qualified staff. Incidents should be reported via the Safeguard system. Where it is deemed sufficiently serious, the Serious Untoward Incident procedure will be invoked.

96. Access Control to Systems

97. Staff will not be given access to an information system unless properly trained and made aware of their security responsibilities.

98. All users will keep passwords, key-codes etc. secret. Managers shall ensure that appropriate procedures and staffing levels are in place to cater for absence.

99. All staff using any of the Connecting for Health suite of applications will require an individual smartcard issued by the Trust Registration Authority. The conditions of use are described on the application form RA001. A copy is available on the Trust Intranet.

100. Housekeeping

101. Information should be stored securely when not in use as indicated by risk assessment. Computer equipment shall not be left logged on when unattended. Fax machines should be located within secure areas.

102. Information systems will have documented backup regimes. Secure storage will be used. Such storage shall be geographical separate from the system location to protect against loss.

103. Information Validation

104. Information accuracy is the direct responsibility of the person inputting the data supported by their line manager.

105. Any loss or corruption of information shall be reported to the relevant information systems manager at once.

106. Systems must incorporate internal validation process and audit trails to record transactions.

107. Audit trails will be interrogated where necessary in the course of an investigation.

108. Virus Control

109. The Informatics department will take all reasonable steps to minimise the risks of computer viruses entering the Trust's network and systems.

110. Users must take reasonable care when accessing web sites and connecting devices to their PC to avoid downloading viruses.

111. The Informatics department will ensure that all PCs, thin client desktop devices, mobile devices and servers will have up to date virus protection software.

112. Users shall report any viruses detected/suspected in the system immediately to the IT Service Desk.

113. Equipment Asset Control

114. The Informatics department will keep an asset register of the type and location of all IT equipment assets in accordance with the Trust's financial regulations.

115. Register of Information Assets

116. A register of information assets held shall be maintained by each directorate classified by sensitivity and criticality in accordance with the requirements of the Freedom of Information Act.

117. Personnel – Security Standards

118. Provision for the inclusion of confidentiality agreements in contracts of employment shall be made by the Human Resources Directorate.

119. All terms and conditions of employment issued to Trust staff shall indicate employee's responsibility for information security.

120. Training on data security and confidentiality forms part of the staff induction process.

121. Specialist advise and training and updating shall be provided as appropriate.

122. Web Site

123. The author of any material uploaded to the Trust's web site is responsible for ensuring factual accuracy and authenticity.

124. Business Continuity Plan

125. The Trust and departments within it shall maintain a business continuity plan for information assets.

126. Particular attention shall be given to the protection of information and communication systems.

127. **Monitoring and Review**

Minimum requirement to be monitored	**Process for monitoring e.g. audit**	**Responsible individual/ group/ committee**	**Frequency of monitoring**	**Responsible individual/ group/ committee for review of results**	**Responsible individual/ group/ committee for development of action plan**	**Responsible individual/ group/ committee for monitoring of action plan**
Access Control	Audit	IAO	Annual	IG Committee	IG Committee	Informatics Committee
Incident Reports	Audit	IG Manager/SIRO	Quarterly	IG Committee	IG Committee	Informatics Committee

128. **Related Policies**

129. The Trust has published discrete policies on:

- Email and Internet usage
- Data Protection Act 1998
- Information Technology Procurement

130. These policies and other such policies as shall be published from time to time and shall be regarded as forming part of this policy document.

Appendix A

Bolton NHS Foundation Trust

ACKNOWLEDGEMENT FORM EM-1

As an employee of Bolton NHS Foundation Trust, I recognise and understand that the Trust's E-mail and access to the Internet system is to be used for conducting business in compliance with Trust policy and that the Trust may monitor e-mails and internet access.

I agree not to disclose any passwords, access tokens or other security arrangements.
I am aware that violations of this Policy may subject me to disciplinary action.

The Trust's IT Security and Email Usage policy can be found at
http://www.boltonft.nhs.uk/about-us/freedom-of-information/publication-scheme

I acknowledge that I have read and understood the Trust's Policy regarding the use of E-mail and Internet usage.
*** All fields must be completed**

PLEASE COMPLETE THE BELOW FORM IN CAPITAL LETTERS

*** Managers Name (Required):**

*** Full Name:**
(e.g. DAVID MARK SMITH) _____.

*** Job Title:**
_____.

*** Department:**
_____.

*** Location:**
(e.g. Health Centre, Ward) _____.

*** Directorate / Division:**
_____.

*** Telephone (Work):**
_____.

*** Employment Start Date:**
_____.

*** Signed:**
_____.

*** Date Signed:**
_____.

Have you previously or do you currently have a role at the Trust? **Yes** **No**
If yes, please complete the second page of this form.

Please Note: If the form is incomplete or not completed accurately we will not be able to create your account, delaying your access to the trust's IT systems. If you are unsure of any information, please contact your manager for assistance.

PREVIOUS JOB ROLE DETAILS

ONLY COMPLETE: If you have previously worked for the trust or currently have another role at the trust, please complete the following details for that role:

*** All fields must be completed**

*** Job Title:** _____.

*** Department:** _____.

*** Location:**
(e.g. Health Centre, Ward) _____.

*** Directorate / Division:** _____.

*** Telephone (Work):** _____.

*** Employment Start Date:** _____.

Appendix B

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	

131.