Barnet, Enfield and Haringey NHS
Mental Health NHS Trust

A University Teaching Trust

Internet Policy

Version:	5
Policy Number:	IG 03
Policy Lead/Author & Position:	Chief Information Officer
Responsible Directorate:	Information Governance
Replacing Document:	Version 4
Approving Committee / Group:	Information Governance Group
Date Approved/Ratified:	July 2012
Ratified by:	Policy Development, Review and Monitoring Group
Previous Reviewed Dates:	Jan 2006, Sept 2009, Aug 2012, Oct 2015
Date of Current Review:	Feb 2018
Date of Next Review:	Feb 2021
Relevant NHSLA Standard / CQC Outcome(s):	Nil
Target Audience	All staff

EQUALITY STATEMENT

Barnet, Enfield and Haringey NHS Trust aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account its legal obligations under Equality Act 2010, the Human Rights Act 1998 and other relevant legislation.

This document has been assessed to ensure that no one affected will receive less favourable treatment on the basis of a protected characteristic - age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex (gender) and sexual orientation.

The Trust embraces the four staff pledges in the NHS Constitution and this policy is consistent with these pledges. The Trust is also committed to safeguarding and promoting the welfare of children, young people and vulnerable adults and expects all staff and volunteers to share this commitment.
The Trust will make accessible versions of this document available if requested by members of the public, service users or staff who have particular communications needs.

Trust Values

This Policy supports the BEHMHT Trust values of:

- **Compassion.**
- **Respect**
- **Working Together**
- **Being Positive**

Version Control Summary

Version	Date	Section	Author	Comments
3	15/08/12	All sections	IG Lead	Policy now in NHSL format. HIS have been replaced by HP. Additional definitions added.
4	21/09/15	Sections 5, 10, 13, 14 & 15		Changes to accountabilities, amendments made in accordance with organisation structure, paragraph added to raise awareness related to Trust accessing information relating to Internet use. Guidance related to use of internet by service users added. HP duties amended, reference to non-existing organisations brought up to date, additional references added.
5	26/02/18	Various sections	Data Protection Officer	Changes made in preparation for new data protection legislation (GDPR)

Table of Contents

1 Introduction

Barnet, Enfield & Haringey Mental Health NHS Trust (the Trust) are committed to the use of the Internet to support specific clinical and business purposes In doing so it must ensure that suitable controls are in place to prevent security breaches or other negative consequences. The networks used for the Internet are not secure and any communication sent by this means could be accessed or modified by unauthorised individuals. There are also threats from obtaining information from the Internet, with virus attachments being the most common.

2 Purpose & Aim

The purpose and aim of this policy is to:

Ensure the Trust adopts procedures to minimise the risk of using the internet and follow good practice in the way users behave and the Internet sites that they visit.

3 Scope and Outcome

This policy applies to all Trust employees whether on a permanent contract, a member of the bank or agency staff.

4 Definitions

Encryption - Encryption is the conversion of data into a form, called a cypher text that cannot be easily understood by unauthorised people

Cypher text is encrypted text

Decryption - is the process of converting encrypted data back into its original form, so it can be understood

Firewall – A firewall can either be software-based or hardware-based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analysing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. A network's firewall builds bridge between an internal network that is assumed to be secure and trusted, and another network, usually an external (inter)network, such as the Internet, that is not assumed to be secure and trusted.

Copyright - Copyright is a legal concept, enacted by most governments, giving the creator of an original work exclusive right to it, usually for a limited time.

5 Duties

Chief Executive - is responsible for the Trust having appropriate strategies and structures in place for the protection of its systems.

Senior Information Risk Owner (*SIRO).* The SIRO has overall responsibility for managing information risk and ensuring data is adequately protected across the Trust. The SIRO is the policy lead for information governance risk which includes staff use of the internet,

Managers - All managers are responsible for ensuring the staffs that they manage are aware and familiar with this policy, either through local induction and/or one to one supervision meetings.

Managers are responsible for ensuring all staff have completed the relevant IT security declaration document prior to agreeing access to the Trust network, this includes managers countersigning the declaration indicating they have checked the member of staff is aware of their responsibilities within this policy. Managers are also responsible for ensuring that staffs within their service are aware of their responsibilities in relation to providing staff with information about the standards of acceptable use

Account Security Officer – will manage the Internet and Firewall facilities and will be responsible for reporting any suspected breach of security to a satisfactory conclusion. **THE TRUST'S NETWORK PROVIDER** service desk will be responsible for ensuring that effective access control is implemented in accordance with defined procedures so that only authorised users may access the information.

Data Protection Officer (DPO) is accountable to the Chief Information Officer. The role of the DPO is to inform and advise and monitor the Trust and its employees about their obligations to comply with data protection laws. The DPO will be the first point of contact for supervisory authorities such as the Information Commissioner and for individuals whose data is processed (employees, customers etc.).

Employees – All Trust employees are personally responsible for ensuring they comply with this policy.

Waiver

Employees, students and any other persons acting under the authority of the Barnet, Enfield & Haringey Mental Health NHS Trust should endeavour to ensure their full compliance with Internet Policy at all times. Any variation from this Policy's guidance, recommendations and/or rulings lies at the discretion of the Chief Executive of the Trust and the Director of the Trust's network provider.

6 INTERNET USAGE

- The Trust has established that Internet access for personal use is permitted during breaks.
- Where clinical and business-specific material is obtained from the Internet, users must ensure that any copyright restrictions are obeyed and that virus protection procedures are followed.
- The Internet must never be used for the communication of confidential information, even where encryption technology is available. Moreover, the Internet should not be used as a communication medium where any commitment is made on behalf of the Trust or where commitments are received e.g. from suppliers.
- When sending e-mail communications, it must be ensured that the content does not contain any material of a confidential or defamatory nature, or engage in any racial or gender based abuse. The content of e-mails could be used within legal action and the same caution should be exercised as with the written medium (see the Trust's email policy for further information).

  The internet should not be used for personal media streaming e.g. radio, television, etc. as this has the potential to impact on the network performance

7 INFORMATION PUBLISHED ON THE INTERNET

Where material owned by The Trust is published on the Internet, it must bear copyright markers, and must be registered under the Copyright Act

Published contact information must be centrally managed.
Information published by the Trust on the Internet:

- Must not incite or promote illegal acts;
- Must be legal, decent, honest and truthful;
- Must not deliberately or negligently mislead the reader; and
- Must have a disclaimer attached to the document.

Links to external sites should be verified to ensure that the link target page is valid and is not presenting information likely to offend, preventing the inadvertent viewing of unsuitable material.

8 RESPONSIBILITIES FOR SECURE OPERATING PROCEDURES

Suspected or detected security breaches must be reported to the Data Protection Officer and the Service Desk, who will record and investigate all reported breaches of security to a satisfactory conclusion.

The service desk will be responsible for ensuring that effective access control is implemented in accordance with defined procedures so that only authorised users may access the information.

The service desk will ensure that the Information Security Manager can access the contents of the Internet audit trails each month to record and report any inconsistencies for investigation.

9 SECURE OPERATING PROCEDURES

In suspected cases of abuse, the Trust's network provider will immediately report the incident in accordance with the Trust's IG Incident Management Policy.

The Trust's network provider will manage the Internet and Firewall facilities in order to ensure that, wherever possible:

- The Firewall protects the internal network from unauthorised access;
- The Firewall blocks access to any IP address known to carry inappropriate or illegal material.

10 INTERNET USERS

Users who breach this Internet Policy may be liable to disciplinary action under the Trust's disciplinary procedure.

Users should be aware that the Trust's internet service retains records of all sites visited by each user and this information may form part of any investigation into staff's use of Trust provided IT facilities.

Users will not make use of the Internet for personal financial gain.

Users who deliberately access sexually explicit images, store or make such images available on storage medium owned by the Trust, this will result in disciplinary action under the Trust's disciplinary procedure.

Users will not make use of the Internet to engage in activities that are of questionable legality such as on-line gambling or posting information that may tend to disparage or harass others on the basis of gender, race, age, disability, religion, sexual orientation or national origin etc.

Users of the Internet will not participate in chain letters; post statements that are defamatory or information that is false or misleading; or post confidential or proprietary information about the Trust or any of its patients, staff or clinical and business associates on unsecured Internet sites such as bulletin boards, or disseminate such information in a way that might compromise its confidentiality.

Users of the Internet will not download, use or distribute copyrighted materials from the Internet without proper authorisation from, and/or payment of, applicable user fees to the owner of the intellectual rights of such copyrighted materials.

Users will not make use of the Internet for any purpose which might be considered to contravene any existing laws of England and Wales.

Users must always exit out of the Internet whenever work has been completed.

Users must never leave their desktop PC unattended when not at their workstation unless using a time-out screensaver or logging out of the system.

Perceived breaches of security (actual or attempted) must be reported to the Data Protection Officer.

- **Service Users**

Mobile computing devices provide a readily available means of communication with family and friends and are in widespread use. It is unlikely to be appropriate to impose a blanket restriction banning their use except in units specifically designed to provide enhanced levels of security in order to protect the public. Blanket restrictions may breach Article 8.

Trust computers with internet access are available in several patient common rooms but it prohibits access to illegal or what would otherwise be considered inappropriate material, eg pornography, gambling or websites promoting violence, abuse or hate. These computers permit the use of social media such as Skype but can be restricted if not used appropriately or if its use is deemed a clinical or security risk.

Staff should remind patients of confidentiality requirements and the implications of breaching patient and staff confidentiality, and encourage patients to consider what they post on social media.

The Trust's network provider will:

- Provide usage reports for the internet facilities based on authorised requests
- Produce reports of Internet security for senior management as requested or if thought necessary for any specific incident.

11 Associated Trust Documents

Email Policy
Information Governance Policy
Information Sharing Policy
Information Security Policy
Information Risk Policy
Records Management Policy
Visitors Policy

12 Monitoring Compliance and Effectiveness

Service Line Clinical Directors/Assistant Clinical Directors/Managers are responsible for disseminating and implementing this policy and to identify learning and development requirements and to incorporate them in to Personal Development Plans and the review of those. In the event of a suspected breach of these procedures, the Trust may initiate further measures, such as disciplinary procedures

13 Dissemination and Implementation

This document will be made available to all Trust staff on the Trust Intranet and through line management cascade and brought to the attention of new staff via the induction process. The policy will also be disseminated through bi-monthly Policy update and " Take 2 ". This policy supersedes all previous policy implementation.

14 Training

Information Security training is included in the Trust's annual mandatory training plan. All staff is required to undertake training by means of the NHS Digital ELearning Information Governance training tool or an alternative approved method of learning.

15 Contributors

Information Governance Manager
Information Security Manager (DXC)
Information Governance Group
Policy Development and Review Committee

16 References

This policy has been prepared in reference to the documents listed below and should be read in conjunction with them, and are available on the Trust intranet http://staff.beh-mht.nhs.uk/

- General Data Protection Regulation and Caldicott principals
- Department of Health Confidentiality NHS Code of Practice
- Department of Health Information Security Management Code of Practice
- NHS Digital
- Information Commissioner's Office

17 Appendix 1

GUIDELINES FOR INFORMATION SECURITY ON THE INTERNET

INTRODUCTION

The use of the Internet has grown astonishingly quickly in recent years. Nowadays, many professionals are extensive users of the technology, and indeed would feel they could not function effectively without ready access to it. What is not so readily appreciated is that the Internet gives rise to a large number of issues in regard to Data Protection. The law imposes a discipline on creators and recipients of Web pages that is at odds with the relaxed, informal style associated with the technology. In this section, some of the Data Protection problems associated with the Internet are described and recommendations are made for good practice.

THE INTERNET AND THE DATA PROTECTION ACT

Where Web pages contain personal information, hypertext links displaying personal information, or where the individual user is identified using log pages, the Web pages are subjected to Data Protection legislation. Processing other than by reference to the data subject (patient or staff) will now be covered by Data Protection legislation (this type of processing was specifically excluded from the remit of the 1984 Act), meaning that many more Web pages will be governed by new legislation. Personal information that is contained in Web pages should be treated in the same way as any other form of written communication regarding Data Protection.

FAIR AND LAWFUL PROCESSING - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject

Personal information on Web pages should be capable of passing the same tests as that of any other material regarding fair and lawful processing. The First Principle of The General Data Protection Regulation includes a requirement for an individual to be told of the identity of the data controller (i.e. The Trust) and the purposes for which his/her data is intended to be processed (i.e. uploaded onto the Internet). Where a Web page contains a link to send an email to a person in a department or organisation, then it is appropriate to indicate that the email will be processed in a specific manner in accordance with the law.

WEB PAGES THAT ARE ADEQUATE, RELEVANT AND NOT EXCESSIVE

As with any processed data, the content of any Web page must only reflect the amount and nature of information specifically needed for that Web page. Appropriate guidance, regulation and supervision mechanisms need to be put in place to ensure this.

WEB PAGES THAT ARE ACCURATE AND UP-TO-DATE

As with any processed data, the content of Web pages must be accurate and up-to-date. As much care must be taken over the reliability and accuracy of information in Web pages as in any other documentation being used by The Trust. The semi-formal and transient qualities associated with the Internet should not lure users into regarding the content (particularly in terms of accuracy) as unimportant.

In addition, as Web pages may not necessarily be updated regularly, then their age and supervision mechanisms need to be in place to ensure that obsolete information is not treated as current.

RIGHTS OF THE DATA SUBJECTS (PATIENTS AND STAFF)

The rights accorded to data subjects apply to Internet and email as they do to any other processed data. Specifically, there is the right to be informed of processing. Furthermore, the data subject is entitled to be told the purposes for which the data is processed and any further information which is necessary to make the processing fair. Should Web pages identify individuals (i.e. staff and patients), then The Trust should seek consent before publishing that information. Data subjects have the right to prevent processing in certain circumstances, and the right to block or erase data about them. It is important not to overlook email address lists and messages, as they too are covered by the Data Protection legislation.

INFORMATION SECURITY

Attention to security is a fundamental aspect of Data Protection management and the Internet is no exception. Web pages are vulnerable to security breaches as they can be intercepted and altered by a third party. Therefore, The Trust should investigate the security of Web pages and adopt appropriate security arrangements and management regimes. Furthermore, printed material from the Internet (i.e. paper printouts) will also be treated as personal information by the Data Protection legislation, so mechanisms to protect manual information is equally important.

INTERNET MANAGEMENT REGIMES

The Internet has become an integral component of The Trust's communication and an excellent source of information. Nurturing good Internet practice is sound business sense whatever the circumstances. It becomes an even greater imperative where the legal pitfall surrounding inappropriate use of the Internet is concerned. In addition to Data Protection, there is potential for the contents of Web pages to fall foul of legislation relating to such areas as defamation, racial abuse, harassment and obscenity. A good Internet practice culture will need to be developed by The Trust to ensure total compliance with legislation.

GOOD INTERNET PRACTICE

- Web pages should be created within the terms of Notification under Data Protection legislation.
- Web pages should only use personal information if necessary.
- Web pages should be concise.
- Web pages should work to a high level of accuracy in terms of content.
- The Trust should work on the basis that all personal information in Web pages may be inspected by a data subject.
- The Trust should work on the basis that all Web pages will be audited for compliance with the law and organisational policy.
- The Trust should work on the basis that email transactions will be audited for compliance with the law.
- The Trust should not keep paper copies of Web pages as far as is practical.
- The Trust should initiate regular weeding of redundant pages that are no longer used.
- The Trust should work on the basis that consent from Data Subjects must be received before publishing their information on any Web page.

MONITORING COMPLIANCE WITH AND EFFECTIVENESS OF PROCEDURAL DOCUMENTS FORM

1.	**How will the document Be monitored? (please circle as appropriate)**	**Audit**		**Review**	**Other, please specify;**
		Methodology:			
2.	**What is the process for reviewing results of Monitoring?**	Discuss at IG Meeting			
3	**Report to:**	**SIRO**			
4.	**Who is responsible for conducting the Monitoring? (please circle as appropriate)**	**Group / Committee**		**Individual**	
		Name / Title (also include position of individuals): IG Forum			
5.	**How often will the document be Monitored? (please circle as appropriate)**	**Monthly**	**6 Monthly**	**Yearly**	**Other, please specify;**
		Comments: To be reviewed 3 yearly or when necessary due to changes in guidance			
6	**Responsibility for action planning after review**				

EQUALITY IMPACT ASSESSMENT AND ANALYSIS FORM

1. Please indicate the expected impact of your proposal on people with protected characteristics					
Characteristics	Significant +ve	Some +ve	Neutral	Some -ve	Significant-ve
Age:			Y		
Disability:			Y		
Ethnicity:			Y		
Gender re-assignment:			**Y**		
Religion/Belief:			**Y**		
Sex (male or female)			**Y**		
Sexual Orientation:			**Y**		
Marriage and civil partnership			**Y**		
Pregnancy and maternity			**Y**		
The Trust is also concerned about key disadvantaged groups event though they are not protected by law					
Substance mis-users			**Y**		
The homeless			**Y**		
The unemployed			**Y**		

2. Consideration of available data, research and information

Monitoring data and other information should be used to help you analyse whether you are delivering a fair and equitable service. Social factors are significant determinants of health outcomes. Please consult these types of potential sources as appropriate. There are links on the Trust website:

- **Joint strategic needs analysis (JSNA) for each borough**
- **Demographic data and other statistics, including census findings**
- **Recent research findings (local and national)**
- **Results from consultation or engagement you have undertaken**
- **Service user monitoring data (including age, disability, ethnicity, gender, religion/belief, sexual orientation and)**
- **Information from relevant groups or agencies, for example trade unions and voluntary/community organisations**
- **Analysis of records of enquiries about your service, or complaints or compliments about them**
- **Recommendations of external inspections or audit reports**

	Key questions	Reference data, research and information that you have reviewed which you have used to form your response

2.1	**How does this change/development/plan relate to the Trust's corporate equality Objectives and the public sector duty?**	Any changes are made in accordance with the Health & Social Care Information Centre, Code of Practice on Confidential Information http://systems.hscic.gov.uk/infogov/codes/cop
2.2	**What are the relevant equalities characteristics of the staff involved or Affected?**	NA
2.3	**What are the relevant equalities characteristics of the service users and Carers involved or affected?**	NA
2.4	**What other relevant data do you have in Terms of service users or staff? (e.g. results of customer satisfaction surveys, consultation findings, census data, and health needs assessments Etc.).**	**Health & Social Care Information Centre, Code of Practice on Confidential Information** http://systems.hscic.gov.uk/infogov/codes/cop **Information Commissioner's office website** https://ico.org.uk/

3. Equality Impact Analysis Improvement Plan

If your analysis indicates some negative impacts, please list actions that you plan to take as a result of this analysis to reduce those impacts, or rebalance opportunities. These actions should be based upon the analysis of data and engagement, any gaps in the data you have identified, and any steps you will be taking to address any negative impacts or remove barriers. The actions need to be built into your service planning framework. Actions/targets should be measurable, achievable, realistic and time framed.

Issues identified	Actions required	By who

4. Sign off and publishing

Once you have completed this form, it needs to be 'approved' by Service Director, Clinical Director or an Executive Director or their nominated deputy. If this Equality Impact Analysis relates to a policy, procedure or protocol, please attach it to the policy and process it through the normal approval process. Following this sign off by the Policy Review and Monitoring Committee your policy and the associated EqIAn will be published by the Trust's policy lead on the website.

If your EqIAn related to a service development or business /financial plan or strategy, once your Director or the relevant committee has approved it please send a copy to the Equalities Team (equalities@beh-mht.nhs.uk), who will publish it on the Trust's website. Keep a copy for your own records.

I have conducted this equality Impact analysis in line with Trust guidance

Your name: Doreen Todd	**Position: Information Governance Manager**
Signed: 	**Date:**

Approved by:	
Your name:	**Position**
Sign:	
Date	