Acceptable Use of ICT Policy

During the COVID19 crisis, please read the policies in conjunction with any updates provided by National Guidance, which we are actively seeking to incorporate into policies through the Clinical Ethics Assurance Group

Document Author	Authorised
Written By: Information Security Manager **Date:** October 2019	**Authorised By:** Chief Executive **Date:** 19th March 2020
Lead Director: Director of Finance, Estates and IM&T	
Effective Date: 19th March 2020	**Review Date:** 18th March 2023
Approval at: Policy Management Sub Committee	**Date Approved:** 19th March 2020

DOCUMENT HISTORY

(Procedural document version numbering convention will follow the following format. Whole numbers for approved versions, e.g. 1.0, 2.0, 3.0 etc. With decimals being used to represent the current working draft version, e.g. 1.1, 1.2, 1.3, 1.4 etc. For example, when writing a procedural document for the first time – the initial draft will be version 0.1)

Date of Issue	Version No.	Date Approved	Director Responsible for Change	Nature of Change	Ratification / Approval
8 Feb 15	0.1		Transformation and Integration	Initial Draft	
26 Feb 2015	0.2		Transformation and Integration	Post Seniors Comments	
23 Mar 2015	0.3		Transformation and Integration	Comments following	IGSG
01 Apr 15	0.4		Transformation and Integration	Incorporated comments from	Ambulance, Comms and IM&T DG
29 Nov 2016	0.5		Director for Strategy and Planning	Minor updates	
08 Dec 2016	0.5		Director for Strategy and Planning	For ratification	Information Governance Steering Group
13 Dec 2016	0.5		Director for Strategy and Planning	For Approval	Corporate Governance & Risk Sub-Committee
21 Dec 2016	0.6		Executive Director Strategy and Planning, ICT and Estates	Incorporate minor comment from staff side representative	Corporate Governance & Risk Sub-Committee
21 Dec 2016	0.6		Executive Director Strategy and Planning, ICT and Estates	Out on Voting buttons for Approval	Corporate Governance & Risk sub-Committee
10 Jan 2017	1	10 Jan 2017	Executive Director Strategy and Planning, ICT and Estates	Approved via voting buttons at	Corporate Governance & Risk sub-Committee
23 Oct 19	1.1		Director of Finance, Estates and IM&T	Endorsed via voting buttons at	Information Governance Sub-Committee
19 March 2020	2.0	19 March 2020	Director of Finance, Estates and IM&T	Approved via voting buttons and Chairs approval at	Policy Management Sub-Committee

NB This policy relates to the Isle of Wight NHS Trust hereafter referred to as the Trust.

Contents

1. Executive Summary 4
2. Introduction 4
3. Definitions 4
4. Scope 5
5. Purpose 5
6. Roles and Responsibilities 5
7. Policy detail/Course of Action 6
8. Implementation 18
7 Consultation 18
8 Training 18
9. Monitoring Compliance and Effectiveness 19
10. Links to other Organisational Documents 20
11. References 20
12. Appendices 20

1. Executive Summary

1.1 This Policy sets the 'ground rules' for the acceptable use of Information Technology systems and services owned and operated by Isle of Wight NHS Trust. It applies to all the Trust's staff, together with those working for or on behalf of the Trust, including sub-contractors.

1.2 This policy describes the responsibilities and acceptable use of ICT and Information assets within the Trust.

2. Introduction

2.1 The policy covers the following areas for acceptable use:

- Responsibilities and use of ICT assets
- Use of e-mail and Internet
- Use of mobile devices, removable media and remote access
- Network usage (Including passwords/user access control)
- User declaration

2.2 All staff will be required to read this policy as part of their mandatory annual Data Security Awareness Training and be appropriately authorised by their manager prior to gaining access to the ICT network. Visiting and other temporary staff will be required to read and sign a copy of the policy before being given account credentials. All updates to the policy will be communicated to staff via the e-bulletin.

2.3 Access to the National NHS network and National applications including NHSmail will also be subject to the NHS terms and conditions of use and their acceptable use policy.

3. Definitions

3.1 **Information Asset**: This may be patient data, employee information or other information held by the Trust. But it is not only about personal information. It includes any type of information that, if lost or misused, could affect our ability to deliver services, or could damage the Trust's reputation. The information asset is also the device,system or process which the information is processed

3.2 **Confidentiality:** Ensuring that personal, sensitive and/or business critical information is appropriately protected from unauthorised access and can only be accessed by those with an approved role based need to access information relevant and proportionate for the purposes required.

3.3 **Integrity:** Ensuring that information has not been input incorrectly, corrupted or falsely altered or otherwise changed such that it can no longer be relied upon.

3.4 **Availability:** Ensuring that information is available at point of need to those authorised to access that information.

3.5 **Malware:** Software intended to cause harm or disruption to computers or networks. There are many classifications of Malware (MALicious softWARE) but as a general term it deals with all forms of viruses, spyware, Trojans and other software designed with malicious intent.

3.6 **Spam:** Mass unsolicited electronic mail received from an un-requested source which attempts to convince the user to purchase goods or services. SPAM consumes valuable network resources while delivering no business benefit.

3.7 Blogging or Tweeting: This is using a public website to write an on-line diary (known as a blog) or sharing thoughts and opinions on various subjects. Blogs and Tweets are usually maintained by an individual with regular entries of commentary, descriptions of events, and may include other material such as graphics or video Examples of blogging websites include Twitter.com and Blogging.com.

3.8 Social Media: 'Social Media' is the term commonly given to web-based tools which allow users to interact with one another in some way, by sharing information, opinions, knowledge and interests online. As the name implies, social media involves the building of online communities or networks to encourage participation and engagement. There are a large range of social media platforms available which continue to expand and increase including:

- Social networking – e.g. Facebook
- Professional networking – e.g. LinkedIn
- Video blogging – e.g. YouTube
- Microblogs – e.g. Twitter
- Blogs – e.g. Wordpress
- Social media can include; blogs, audio, video, images, podcasts and other multimedia communications.

3.9 Social Networking: This is the use of interactive web based sites or social media sites, allowing individuals on-line interactions that mimic some of the interactions between people with similar interests that occur in life. Popular examples include Facebook.com and Linkedin.com.

3.10 Social Engineering or Blagging: This is the method whereby an attacker uses human interaction (social skills) to deceive others to obtain information about an organisation and its information assets including personal data. An attacker may potentially masquerade as a respectable and plausible person claiming bona fide interest in the information concerned e.g. posing as a member of the organisation's staff or maintenance contractor etc.

4. Scope

4.1 This policy applies to Isle of Wight NHS Trust, referred to as the 'Trust', and includes all hospital, units and community health services managed by the Trust.

4.2 This policy applies to all those working for or at the Trust, in any capacity. A failure to follow the requirements of the policy may result in investigation and disciplinary action.

5. Purpose

5.1 This policy sets out the responsibilities and acceptable use of ICT and information assets within the Trust.

6. Roles and Responsibilities

6.1 Senior Information Risk Owner (SIRO):

6.1.1 The SIRO has overall responsibility for all The Trust's Information assets and for ensuring that information risks are mitigated effectively, and as such is responsible alongside the Director with responsibility for ICT for ensuring that this policy is in place and adhered to.

6.1.2 The Trust's Senior Information Risk Owner (SIRO), takes ownership of the risk management of information assets and reports as appropriate to the Trust Board.

6.2 Information Asset Owners (IAO's):

6.2.1 IAO's are operationally responsible at senior level for all information assets within their business areas. IAO's should understand and address the levels of risk in relation to the business assets they own and provide assurance to the SIRO on the security and use of those assets on at least an annual basis.

6.3 Information Asset Administrators (IAA's):

6.3.1 IAA's work at local business/departmental level and ensure that system administration and security procedures are in place for all information assets and that these are followed, recognised and report actual and potential security incidents, liaise with the IAO on incident management and ensure the information asset register is accurate and up to date.

6.4 ICT Service:

6.4.1 The ICT services department is responsible for maintaining the hardware and software components of the ICT infrastructure and, implementing all necessary technical and physical security controls.

6.5 Information Communication Technology Programme Group:

6.5.1 The Information Communication Technology Programme Group is a formal working group to oversee and coordinate the technical and organisational security measures that need to be place for all the key Information assets to ensure the confidentiality, integrity and availability of information in line with the ISO 27001 Information Security Standard.

6.6 All Managers:

6.6.1 All managers are directly responsible for implementing policies and procedures within their business areas.

6.7 All Staff:

6.7.1 It is the responsibility of each employee to adhere to policies and procedures and undertake Data Security Awarness training on an annual basis via the Trust mandatory training and e-learning

7. Policy detail/Course of Action

7.1 Acceptable Use of Information Assets

7.1.1 Staff may only use information assets, which are specifically authorised by their line manager, in accordance with this policy. Unauthorised use, modification, removal of information assets is strictly prohibited. Where information assets are needed to be removed off-site, management approval for the removal of such information assets must be obtained (this applies to paper, hard copy and other forms of media). Records stating management approval for the removal of information assets will need to be maintained.

7.2 All users and the Trust are subject to the provisions of the:

- General Data Protection Regulations 2016/679 (GDPR)
- Data Protection Act 2018

- Access to Health Records Act 1990
- The 10 NHS Data Security Standards
- Computer Misuse Act 1990
- Human Rights Act 1998
- Copyright, Designs and Patents Act 1988
- Freedom of Information Act 2000
- Privacy and Electronic Communications Regulations 2019
- Regulation of Investigatory Powers Act 2000
- Defamation Act 1996
- Obscene Publications Act 1959
- Protection of Children's Act 1978
- Equality Act 2010

7.3 Copies of these Acts and guidelines are made available via http://www.legislation.gov.uk and the Trust's Intranet.

7.4 Acceptable Use of Email and the Internet

7.4.1 The Trust views the Internet and e-mail as essential tools for all their staff. However, their use can expose the Trust to technical, commercial and legal risks if they are not used sensibly and lawfully. It can also degrade the performance of the IT infrastructure due to excessive and inappropriate use.

7.4.2 The aim of this policy is to:

- provide direction on your use of the Internet and e-mail at work to minimise the Trust's exposure to these risks;
- explain what you can and cannot do;
- provide some explanation of the legal risks that you need to be aware of in your use of the Internet and e-mail;
- explain the consequences for you and the Trust if you fail to follow the rules set out in this policy.

7.4.3 This policy reflects the Trust's agreed strategy for access and usage of e-mails and the Internet.

7.4.4 This policy is part of a comprehensive code of conduct for all staff.

7.4.5 It is essential that all staff read this policy. Breaches of this policy will be taken very seriously and may lead to disciplinary action. If there is anything you do not understand it is up to you to ask your line manager or the Information Governance Lead and Data Protection Officer to explain.

7.5 Permitted and Prohibited Uses:

7.5.1 You should only access the Internet if such use is required as part of your job, primarily for healthcare related purposes. Limited and reasonable personal use is permitted as long as it does not interfere with the performance of your duties and is authorised by your line manager.

7.5.2 Access to chat lines, bulletin boards, blogs and social networks on the Internet are routinely blocked by the Trust's web filtering software. However, if access is needed

for official Trust use this should be agreed and coordinated via our Communications Department, following approval of your line manager.

7.5.3 You must not use the Internet for any gambling or illegal activity, including for personal business use.

7.5.4 The Trust's may use automated content filtering software to restrict access to categories of websites that are deemed to be inappropriate, e.g. Adult/sexual, violence, criminal, etc.

7.5.5 These are subject to on-going review. However just because you are able to access a particular website may not always mean that it is permitted.

7.5.6 You should only use the Trust's e-mail system for business use, subject to the rules in this policy.

7.5.7 If you do send a personal e-mail, this should be deleted as soon as possible from your mailbox.

7.5.8 Users must not use Trust email for personal business use or illegal activity.

7.5.9 Users must not use and register their Trust email account for non-Trust related services which may lead to unnecessary Spam email being received.

7.5.10 You must not set 'auto-forward' rules for email to your personal or other business email accounts including external NHS mail accounts such as nhs.net or nhs.uk.

7.5.11 You must not transfer person/patient identifiable confidential or business sensitive /confidential information outside the Trust via email or upload to websites unless you are authorised to do so, and that it is absolutely necessary for work purposes and is adequately protected using NHS standard encryption – please see section below for further details.

7.6 Offensive, Illegal and Defamatory Materials

7.6.1 You must not under any circumstances use the e-mail system or internet facilities to access, download, send, receive or view any materials that will cause offence to any person by reason of:

- Any sexually explicit content;
- Any sexist or racist remarks;
- Remarks relating to a person's sexual orientation, gender reassignment, race, ethnicity, political convictions, religion, disability or age.

7.6.2 The Trust's Equality and Diversity Policy applies to e-mail communication. You must comply with the Equality and Diversity Policy.

7.6.3 You must not under any circumstances use the e-mail system or Internet to access, download, send, receive or view any materials that you have reason to suspect are illegal. Please refer to the section 8.3 below "A Guide to the legal Issues relating to use of email and internet" for guidance on what materials may be illegal.

7.6.4 Please remember that it may be illegal to copy many materials appearing on the Internet including computer programs, music, text and video clips. If it is not clear that you have permission to copy materials off the Internet, please do not do so.

7.6.5 You must not send or circulate any materials on the Internet or by e-mail that contain any negative and defamatory remarks about other colleagues and the Trust.

7.6.6 Any use of the e-mail system or Internet access for any of these prohibited purposes will be treated as a serious disciplinary matter which may lead to disciplinary action including the potential of dismissal of the employee concerned.

7.7 Blogging and social networking sites

7.7.1 The use of blogging and social networking websites can expose the organisation to information risks, even where these sites are not accessed directly from work. The popularity of such websites and the rapid growth of internet enabled devices such as mobile phones, blackberries etc. has resulted in significant awareness and uptake of these websites from home, from work and when mobile.

7.7.2 The risks that this may pose include:

- Unauthorised disclosure of business information and potential confidentiality breach.
- Legal liabilities from defamatory postings etc. by staff
- Reputational damage to the Trust
- Staff Intimidation or harassment with possibility of personal threat or attack against the blogger, sometimes without apparent reason.
- Identity theft of personal data that may be posted
- Malicious code and viruses causing damage to IT infrastructure
- Systems overload from heavy use of sites with implications of degraded services and non-productive activities, particularly in the use of rich media (such as video and audio) becoming the norm.

7.7.3 Whilst access to blogging and social networking sites is controlled by the Internet web filter and is only permitted by authorised exception, staff should not attempt to use such sites in work time in consideration of the above risks.

7.7.4 Staff should not have any work related conversations about patients or post defamatory information about colleagues or the Trust to blogging or social networking sites when at home or away from work, as they may be subject to disciplinary action and legal proceedings.

7.7.5 NHS organisations of all types are now making increased use of Social Networking facilities to engage their patients, other stakeholders, and to deliver key messages for good healthcare and patient service generally. These digital interactions are to be encouraged and their values extended as new communications channels become available for use.

7.7.6 The Trust is seeking to make such facilities available so that Trust Communications, Engagement and Membership team will control the Trust corporate social networking messaging to ensure that it is utilised effectively and regularly monitored to improve the content and to remove any inappropriate content.

7.7.7 In future, as improved filters and technology becomes available, staff and stakeholders may be enabled to interact with Trust corporate social networking. This interaction will be managed in consultation with the Trust IG and ICT department.

7.7.8 Please refer to the Trust's Electronic Communications Policy for further information.

7.8 Confidentiality and Sensitive Information

7.8.1 Please remember that email and the internet are not necessarily a secure way of sending information.

7.8.2 You must not use any e-mail system other than NHSmail to send information which is highly confidential or sensitive outside the Trust, as it could cause the Trust loss, damage or embarrassment if it were publicly disclosed, unless you follow these rules:

- It has been agreed as a necessary part of the Trust's service and you have the authority to do so from your department e.g. to the Isle of Wight Council.
- Such information must be adequately encrypted. Please contact ICT services who will advise you on how to encrypt information;
- NHS mail may also be used to communicate securely with other NHS mail user accounts (i.e. @nhs.net to @nhs.net).
- This does not apply to other @nhs.uk email accounts.

7.8.3 You must also not upload person/patient identifiable or confidential or sensitive information to websites unless it is a necessary part of the Trust's service and it is a secure (encrypted) process, which you have authority to undertake.

7.8.4 Please refer to the Information Sharing & Safe Haven Policies for further information.

The following categories of information will be treated as highly confidential:

- Extracts from the Trust's patient databases
- Any Person Identifiable Data (PID) / Personal Confidential Data (PCD)
- Personnel and staff records;
- All information received under a duty of professional confidence from staff or patients.

7.8.5 Please also be aware that e-mail messages, like paper based documents, can be required to be produced in legal proceedings, or in relation to Subject AccessandFreedom of Information Requests.

7.9 Malware, viruses and spam

7.9.1 All Trust computers and laptops should have anti-virus software installed, which is regularly updated via the network or directly from the vendor's website. Emails are also scanned for viruses and malware by the mail servers

7.9.2 Non-text e-mail attachments (e.g. executable files, images etc.) and software downloaded from the Internet may contain computer viruses or other harmful content which can seriously disrupt the Trust's computer systems and network.

7.9.3 Any suspicious emails that may contain malware and viruses should be deleted on receipt. If you believe you may have been infected or compromised, this should be reported as an incident to IT services so that they can be investigated and safely removed, as necessary.

7.9.4 Spam email may contain phishing scams and links to fake websites and should also be deleted on receipt.

7.9.5 If you believe you may have been infected or compromised, this should be reported as an incident to ICT services so that they can be investigated and safely removed, as necessary.

7.9.6 Staff should examine carefully any email coming in to the organisation, including emails from known contacts, as they may be unreliable containing malicious code or spoofed to look as though they are authentic.

7.9.7 Any employee who knowingly distributes a computer virus or any harmful code or spam using the Trust's e-mail system or network will be subject to disciplinary action which may lead to dismissal.

7.10 Security

7.10.1 Do not in any circumstances disclose any user password to any other person.

7.10.2 Do not impersonate any other employee when sending an e-mail and do not amend messages received.

7.10.3 You are responsible for the security of your computer data and e-mail and must not allow use by any unauthorised/other person.

7.10.4 IT systems will be regularly monitored using audit trails and log files to ensure appropriate use and, any misuse will be subject to investigation that may lead to disciplinary action, dismissal and/or criminal proceedings.

7.11 Housekeeping and Good Practice

7.11.1 The following rules will help systems to work more efficiently.

- Messages should be reviewed and deleted on a regular basis and, if necessary, archived in accordance with the NHS Records Management: Code of Practice.
- Where possible, obtain confirmation from the recipient that an important e-mail has been received.
- If you receive a wrongly delivered message you should report this to the sender, and delete the message. If the e-mail message contains confidential or sensitive information you must not make use of that information and must not disclose it.
- Spam or Junk emails should be deleted immediately.
- All-user e-mails must be avoided if possible as they cause system congestion. Messages for a wider distribution should be sent to the Communications Department for onwards distribution.
- Do not subscribe to e-mail services which will result in e-mails being sent automatically to you unless these are for the purpose of your role.
- Do not send out trivial or personal e-mail messages.
- Do not automatically forward messages to other email accounts

7.11.2 Where necessary, users should consider appointing an appropriate deputy to access their email (proxy access) for periods of leave; this deputy should be agreed with your line manager or head of department. Alternatively, users should create an auto reply rule to inform senders to contact an appropriate member of staff if their request needs urgent attention.

7.11.3 In the case of unexpected leave, e.g. long term sick, managers should attempt to obtain consent from the individual to access their email and/or network drive (e.g. H or S drive). If this is not possible managers should seek advice from the Information Governance Lead and Data Protection Officer regarding access to the individuals account. Each case will be assessed individually based on the impact and disruption it may have to the local services.

7.11.4 If a staff member leaves their post or the Trust they should ensure that any data is transferred or proxy access given to an appropriate colleague or their manager, as agreed with your line manager or head of department.

7.11.5 Staff using NHSmail will be subject to its own acceptable use policy and the above arrangements for allowing managers access to staff NHSmail may not be possible.

7.11.6 Note: You should treat e-mail in the same way you would treat a letter or fax.

7.11.7 Do not send any email message that you would not want others to read or to be read out in court.

7.12 Legal Issues relating to use of email and the Internet

7.12.1 This section of the policy is intended to provide staff with information relating to the most important legal issues which may arise from their use of the e-mail system and Internet access.

7.12.2 These are not just theoretical issues. If the law is broken then this could lead to one or more of the following consequences:

- Civil and/or criminal liability for yourself and the Trust.
- Disciplinary action against employees including disciplinary action and potential dismissal.

7.12.3 Ignorance of the law is not a defence in court.

7.13 Bullying and Harassment

7.13.1 The Trust requires all employees to be treated with dignity at work, free from harassment and bullying of any kind. Harassment can take the form of general bullying, or be on the grounds of sex, race, disability, sexual orientation, age, religion. Harassment could include sending sexist or racist jokes, making sexual propositions or general abuse by e-mail. You must not send any messages containing such material.

7.13.2 Bullying and harassment of any kind will be treated as a serious disciplinary matter which may lead to dismissal.

7.13.3 If you are subjected to or know about any harassment or bullying, whether it comes from inside or outside the organisation you are encouraged to contact your line manager/HR advisor immediately.

7.14 Breach of Copyright or Intellectual Property Rights

7.14.1 Materials that you encounter on the Internet or receive by e-mail are likely to be protected by copyright. This will apply to written materials, software, music recordings, graphics, artwork and video clips.

7.14.2 Only the owner of the copyright, or other persons who have the owner's consent, can copy those materials or distribute them.

7.14.3 If you copy, amend or distribute any such materials without the copyright owner's consent, then you may be sued for damages. The Trust may also be liable and, in some circumstances, criminal liability can arise for both you and the Trust.

7.14.4 Be particularly careful not to copy text or download software or music unless you are sure you have permission to do so. Always check the materials in question to see if they contain any written prohibitions or permissions before you copy or download them.

7.14.5 Never download any software, music recordings or other materials that you know to be fakes or “pirate copies”.

7.15 Unwanted Contracts

7.15.1 An exchange of e-mail messages can lead to a contract being formed between you, or the Trust, and another organisation. Contracts can arise easily; all that is required is the acceptance of an offer with the intention that legal obligations should arise and some payment or other consideration being made for the performance of those obligations.

7.15.2 Breach of contract can expose the Trust to a claim for damages.

7.15.3 Contracting by e-mail is subject to the same requirements as any other form of contract. You must adhere to the established policies and procedures about purchasing and contracting.

7.15.4 Never commit the Trust to any obligations by e-mail without ensuring that you have the authority to do so. If you have any concerns that what you are doing will form a contract, contact your line manager. Mark all e-mails relating to contractual negotiations “Subject to Contract”.

7.15.5 You should also ensure that any person with whom you wish to enter into a contract is adequately identified.

7.15.6 Any contract entered into via e-mail must contain the following statement:

“Any contract formed by this e-mail will be governed and construed in accordance with the laws of England and the parties submit to the non-exclusive jurisdiction of the English courts”.

7.15.7 Beware of any attempt by the party with whom you are dealing to incorporate its own terms and conditions into a contract.

7.16 Legal liabilities from defamatory postings by email or internet

7.16.1 If you send an e-mail (NB: even an internal e-mail), or post any information on the Internet/Intranet, which contains any remarks which may adversely affect the reputation of another organisation or person, you will be exposing both yourself and the Trust to the risk of legal action for defamation.

7.16.2 Companies have been sued for the defamatory contents of e-mails sent by employees and have been required to pay out considerable sums as a result.

7.16.3 Legal liabilities may arise where an individual has registered with a site and indicated their acceptance of the sites terms and conditions, which can be several pages long, contain difficult to read legal language and give the site ‘ownership’ and ‘third party disclosure’ rights over content placed on the site. This includes web email accounts. Add-ons installed by additional features or applications can also change the terms and conditions or security features that the user has accepted.

7.16.4 Liabilities may also arise if a user registers with a particular site using a PC within the Trust, as it may be assumed that the user is acting on behalf of the organisation and any libellous or derogatory comments may result in legal action. In addition information being hosted by the website may be subject to other legal jurisdiction overseas.

7.17 Obscene Materials

7.17.1 You must not under any circumstances use the e-mail system or Internet to access, display, circulate or transmit any material with a sexual content (unless relating to their specific clinical role). This may constitute a criminal offence and both the Trust and you personally could be liable. Sexual harassment will be treated as a serious disciplinary matter which may lead to dismissal.

7.18 Protection of Personal Data

7.18.1 Please note that the Trust is required to comply with the Data Protection Act 2018 concerning the protection of personal data. Failure to adhere to that legislation could expose the Trust to civil liability and to enforcement action by the Information Commissioner's Office. Obligations under that legislation are complex but you can help ensure compliance by adhering to the following rules:

- Do not disclose any information about a person in an e-mail or on the Internet which you would object to being disclosed about yourself.
- Be particularly careful when dealing with sensitive information concerning a person's racial or ethnic origin, sexual life, political beliefs, trade union membership, religious beliefs, physical or mental health, financial matters and criminal offences.
- Do not send person identifiable or confidential data using email unless you are authorised to do so and it is encrypted to the required security standard.
- Do not send any person identifiable or confidential data outside the European Economic Area.

7.19 Freedom of Information Act

7.19.1 Emails are deemed to be business records and may be subject to disclosure under the Freedom of Information Act 2000.

7.20 Acceptable use of Mobile Devices, Removable Media and Remote Access

7.20.1 Removable media can be classified as any portable device that can store and/or move data. These include, and are not limited to, Universal Serial Bus (USB) Memory Sticks / Pen Drives, Floppy Disks, Read/Write Compact Disk (CD), DVD, ZIP Drives, Magnetic Tapes, etc.

7.20.2 Mobile devices include tablet PCs, laptops, Personal Digital Assistants (PDA's), mobile phones and blackberry.

7.21 General Rules

7.21.1 In order to prevent damage, compromise or loss of Trust data, the following restrictions will apply to the use of mobile devices and removable media within the Trust:

- Only Trust owned and managed devices should be used to connect to, or synchronise with, the Trust's IT Systems. Privately owned devices must not be used. The ICT department will advise on suitable PDA or removable media devices.
- The device should only be used for work purposes.
- PDA's supplied by the Trust are not permitted to connect to privately owned non-Trust systems.
- Infrared or wireless synchronisation is only to be carried out when it has been specifically agreed and set up by the ICT department.
- Confidential and/or person Identifiable data must not be stored on devices unless it is encrypted to at least 256bit encryption standard. The ICT department can advise on suitable encryption methods.

- The Trust provides encrypted USB sticks for authorised use by staff to transfer any Trust data, including confidential data. However this data should not be transferred and stored on any personal equipment e.g. home PC, laptop or mobile devices (e.g. phones) as they do not offer adequate protection (i.e. encryption) and may lead to unauthorised access of confidential data.
- When transferring data from outside of the Trust, extreme caution must be taken, due to the potential risk of introducing malicious software or viruses on the Trust's IT systems. All data must be virus checked prior to transfer.
- If the media or data is no longer required by the user or the Trust, it should be securely erased and/or disposed of by approved methods by the IT services department.
- All removable media and mobile devices should be stored in a safe, secure environment in line with the Trust security policies and manufacturers recommendations.
- The Trust may use technical measures to enforce restrictions on the use of portable devices and removable media on USB ports and other connecting interfaces.
- Data stored on removable media should be backed up or transferred to the network at regular intervals to ensure compliance with the NHS Records Retention Schedule and mitigate the risk of business disruption.
- Appropriate security measures should be in place to protect the data on any back up media, including encryption of any person identifiable data and secure physical storage.
- All removable media and mobile devices must be returned to the Trust IT services department if the staff member leaves employment or no longer requires it for their job.
- Remote access to the Trust managed networks must be authorised by the Associate Director or Director of the relevant Directorate and approved by the Information Governance Manager. Only Trust-owned laptops can be used for remote access and must be configured with necessary VPN remote access and security software by the ICT department.
- Remote access users should be aware of the security of their connection at any remote location (home, hotel, public hotspot or internet café). It is recommended that home wireless networks are not left on the default or supplier provided settings and should be configured to use Wi-Fi Protected Access 2 (WPA2) and AES encryption to provide the best level of protection.
- Remote access users must ensure the safekeeping of their VPN security tokens and laptops at all times and that the security token is kept separate from the laptop.

7.21.2 Please refer to the Portable Devices and Remote Access Policies.

7.22 Acceptable Network and System Usage

7.22.1 It is the responsibility of all users to ensure that they adhere to the instructions laid down in this policy.

7.22.2 The instructions contained in the policy are special restrictions in force with regard to the Trust related computer systems and network and, are clarifications or additions to the normal security measures in force within the Trust. All usual security precautions must be taken in addition to these specific requirements.

7.22.3 There are also strict NHS security requirements for Trust networks that are connected to the national NHS network by way of mandated compliance with the Information Governance Assurance Statement (IGAS – formerly NHS code of connection).

7.23 Restrictions

7.23.1 Users with access to the Trust's network must not attempt or by their actions or deliberate inaction assist others to attempt:

- Unauthorised access to hardware platforms;
- Unauthorised introduction of software or hardware components to the network;
- Unauthorised modification of network components;
- Unauthorised attempts to access the Trust's network from other networks;
- Unauthorised attempts to access other networks from within the Trust's networks;
- Unauthorised circumvention of security features such as firewalls, passwords, etc.;
- Unauthorised copying or distribution of software, documentation or media associated with the Trust's IT systems;
- Unauthorised removal or relocation of hardware, software, documentation or media associated with the Trust's IT systems.

7.24 File Storage and Housekeeping

7.24.1 Users must store their work in the most appropriate place, giving due consideration to confidentiality and availability.

7.24.2 Documents should not be stored locally (e.g. C: drive) on a desktop computer, laptop or mobile device as they are not backed up and may be irretrievable lost if the device fails or is stolen.

7.24.3 There is also a risk that it may contain person identifiable or confidential data which could get into the wrong hands if lost or stolen.

7.24.4 All new mobile devices (laptops and tablets) must be fully encrypted by the ICT department. Desktop PC's that are not encrypted and located in publicly accessible locations should be either fully encrypted or be physically secured (e.g. securely cabled to desks).

7.24.5 Documents saved to the network shared drive are stored in a secure area and are backed up daily by the ICT department.

7.24.6 Folders on network drives can be restricted to specific staff members. It is advised to store files on departmental shared drives and have the access to the folder restricted by the ICT department for authorised users only. Storing information on departmental drives means that more than one person has access and the information can be retrieved in cases of unexpected leave etc.

7.24.7 Users must keep data storage to a minimum. Delete obsolete files on a regular basis and never store personal non-business related files on the Trust's IT equipment. Files should only be deleted in line with the retention schedules within the Health and Social Care Records Management Code of Practice.

7.24.8 If a staff member leaves their post or the Trust they should ensure that any data is transferred to an appropriate colleague or their manager, as agreed with your line manager or head of department.

7.25 User Access Control and System Usage

7.25.1 The IAAs or system managers are responsible for ensuring that access to IT systems is strictly controlled to authorised users with the appropriate level of access permissions granted and that adequate training is provided prior to access being enabled.

7.25.2 The IAAs must also ensure that access to IT systems is regularly monitored for appropriate use and that any misuse is reported immediately to the relevant line manager, IAO, Information Governance Manager and, may be subject to the Trust's formal disciplinary procedure.

7.25.3 Users must adhere to the following rules:

Password rules:

- Never reveal passwords to anyone;
- Never record or write down their passwords in any form;
- In the event that a password is forgotten, or there are suspicions that it has been discovered by a third party the user should change their password immediately or contact the appropriate system administrator in order to obtain a new password. Use of another individual's account for any purpose, whether or not their password was disclosed in the process, is strictly prohibited and is a disciplinary offense. An incident should be raised if the compromised password has potential to create a data security and protection incident
- Neither the username nor the user's full name should be contained in the password;
- To prevent unauthorised access, all workstations should be secured when left unattended, particularly those in publicly accessible areas. The use of screen lock ('Windows' and 'L' or 'Ctrl', 'Alt' and 'Delete' followed by the 'Return' key), is recommended for short periods of absence and for ward-based accounts where used. Individual user accounts should log off shared computers, if they may be called off, or absent for an extended period, particularly where other staff may need access to the workstation.

General conditions of system use:

- Ensure your user details are accurate and up to date;
- Smartcards that are used for ICT access must be kept safe and secure and not left unattended;
- Users must not to look at any healthcare or personal information relating to themselves, or that relating to family, friends or acquaintances in any circumstances unless directly involved in the patient's clinical care or management. In such circumstances the user must only access relevant and proportionate information if required to as part of their role. They should also make their line manager aware under these circumstances to prevent any potential data breach concerns and consider other options (other staff) to try to negate the need to access the records.
- Users must not maliciously alter, neutralise, circumvent, tamper with or manipulate any part of the system/application components or any access profiles given to them;
- Users must notify the system administrator at any time should any of their access profiles require amendment or should they wish to have their username/password revoked e.g. on cessation of their employment/contracts or other relevant change in their job role.
- Never use or allow anyone else to use a system without authorisation i.e. being issued with an individual username and password and undertaking the appropriate systems training.
- Do not deliberately corrupt, invalidate, deface, damage or otherwise misuse any part of the system/application or information stored by them, including but not limited to the introduction of computer viruses or malicious software that may cause damage or disruption to services.

- Only use any username and password, the system/application and all patient or staff data in accordance with the Trust's Information Governance Policies and Procedures (as available on the Information Governance section on the Trust's intranet), the NHS Confidentiality Code of Practice (as available on www.dh.gov.uk) and (where applicable) in accordance with your contract of employment or contract of provision for service (whichever is appropriate) and with any instructions relating to the system which you are notified of.

7.26 Multifunction Devices (Printer/Scanner/Photocopier/Fax)

7.26.1 Multifunction devices may copy scanned documents and images into its storage disk or memory before printing, which may be permanently retained even if no longer required.

7.26.2 Appropriate security measures should be in place to protect such data from unauthorised access, e.g. use of erasure and encryption incorporated into these devices by the manufacturer, as well as the secure physical location of such devices.

7.26.3 In addition, support/maintenance arrangements for service/repair of the equipment should comply with Trust security policies. Also, any replacement parts that may hold data should be securely deleted and disposed of by the supplier/maintenance company.

7.26.4 Any Multifunction devices with a Public Switched Telephone Network (PSTN) dial-up modem connection that is used for faxing should not be connected directly or indirectly (via PC) to the Trust network, as it poses a serious risk of unauthorised access to the Trust network via the PSTN.

8. Implementation

8.1.1 The responsibility of implementing this policy, including training and other needs that arise shall remain with the author. Line managers have the responsibility to cascade information on new and revised policies/procedures and other relevant documents to the staff for which they manage.

8.1.2 Line managers must ensure that departmental systems are in place to enable staff including agency staff to access relevant policies, procedures, guidelines and protocols and to remain up to date with the content of new and revised policies, procedures, guidelines and protocols.

8.1.3 This document has been compiled by the ICT Department in consultation with the Information Governance Department.

7 Consultation

This document has been reviewed internally by the ICT team and the Information Security Manager.

8 Training

8.2 This policy assumes that staff are IT literate

8.3 General IT training is provided by the Training & Development team.

9. Monitoring Compliance and Effectiveness

9.1 The Trust will regularly monitor and audit its acceptable use practices for compliance with this policy and best practice guidelines.

9.2 The audit will:

- Identify areas of operation that are covered by the Trust's policies and identify which procedures and/or guidance should comply to the policy;
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to processes, and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
- Highlight where non-conformance to the policy is occurring and suggest a tightening of controls and adjustment to related procedures.

9.3 The Trust reserves the right to monitor and inspect any Trust e-mail, Internet access and files at any time without notice. Automated monitoring may take place using audit and security software and intended to ensure that this policy is being adhered to, is effective, and that the Trust and its employees are acting lawfully.

9.4 Permission may be granted to a senior manager with overall responsibility for a particular staff member to access staff email, files or internet logs. This will only be allowed in exceptional circumstances where the individual is suspected of breaching this policy and in cases where disciplinary action is being taken against the individual and it will substantially assist with the investigation. Advice should be sought from the Information Governance Lead and Data Protection Officer and authorisation obtained from an executive director of the Trust.

9.5 However, NHSmail cannot be monitored by the Trust, as it is not owned or managed by the Trust. The Secretary of State for Health is the appointed Data Controller for NHSmail and NHS Directory. Procedures for formal data access requests should be requested from the NHSmail helpdesk.

9.6 Failure to follow the requirements of the policy may result in investigation and management action being taken as considered appropriate. This may include formal action in line with the Trust's Disciplinary and Dismissal Policy and Procedures.

9.7 The results of audits will be reported to the Information Governance Sub Committee, Finance Investment Information and Workforce Committee, Corporate Governance and Risk Management Committee and the Audit Committee, as appropriate.

Monitoring Arrangements	Responsibility / Process / Frequency
Process for monitoring e.g. audit	- Internal Audit - External Audit - Data Security Protection Toolkit
Responsible individual/ group/ committee	Information Communication Technology Dept
Frequency of monitoring	Annually
Responsible individual/ group/ committee for review of results	Information Communication Technology Programme Group
Responsible individual/ group/ committee for development of action plan	Information Communication Technology Programme Group
Responsible individual/ group/ committee for monitoring of action plan	Information Communication Technology Assurance Subcommittee

10. Links to other Organisational Documents

The Remote Working and Portable Devices Policy.

https://www.iow.nhs.uk/Downloads/Policies/Remote%20Working%20and%20Portable%20Devices%20policy.pdf

11. References

https://www.igt.hscic.gov.uk

12. Appendices

Appendix A - Financial and Resourcing Impact Assessment on Policy Implementation

Appendix B - Equality Impact Assessment

Appendix A

Financial and Resourcing Impact Assessment on Policy Implementation

NB this form must be completed where the introduction of this policy will have either a positive or negative impact on resources. Therefore this form should not be completed where the resources are already deployed and the introduction of this policy will have no further resourcing impact.

Document title	Acceptable Use of ICT Policy

Totals	WTE	Recurring £	Non Recurring £
Manpower Costs	N/A		
Training Staff	N/A		
Equipment & Provision of resources	N/A		

Summary of Impact: None identified

Risk Management Issues: None identified

Benefits / Savings to the organisation: None identified

Equality Impact Assessment

- Has this been appropriately carried out? YES
- Are there any reported equality issues? NO

If "YES" please specify:

Use additional sheets if necessary.

Please include all associated costs where an impact on implementing this policy has been considered. A checklist is included for guidance but is not comprehensive so please ensure you have thought through the impact on staffing, training and equipment carefully and that ALL aspects are covered.

Manpower	WTE	Recurring £	Non-Recurring £

Operational running costs	N/A		
Totals:			

Staff Training Impact	Recurring £	Non-Recurring £
	N/A	N/A
Totals:		

Equipment and Provision of Resources	**Recurring £ ***	**Non-Recurring £ ***
Accommodation / facilities needed	N/A	N/A
Building alterations (extensions/new)	N/A	N/A
IT Hardware / software / licences	N/A	N/A
Medical equipment	N/A	N/A
Stationery / publicity	N/A	N/A
Travel costs	N/A	N/A
Utilities e.g. telephones	N/A	N/A
Process change	N/A	N/A
Rolling replacement of equipment	N/A	N/A
Equipment maintenance	N/A	N/A
Marketing – booklets/posters/handouts, etc	N/A	N/A
Totals:	**None**	**None**

- Capital implications £5,000 with life expectancy of more than one year.

Funding /costs checked & agreed by finance:	None
Signature & date of financial accountant:	None
Funding / costs have been agreed and are in place:	None
Signature of appropriate Director or Associate Director:	None

Equality Impact Assessment (EIA) Screening Tool

Document Title:	Acceptable Use of ICT Policy
Purpose of document	This policy sets out the responsibilities and acceptable use of ICT and information assets within the Trust.
Target Audience	All staff and contractors working on behalf of the Trust
Person or Committee undertaken the Equality Impact Assessment	Carl Moreira-Smith

1. To be completed and attached to all procedural/policy documents created within individual services.

2. Does the document have, or have the potential to deliver differential outcomes or affect in an adverse way any of the groups listed below?
   - No
   - If no confirm underneath in relevant section the data and/or research which provides evidence e.g. JSNA, Workforce Profile, Quality Improvement Framework, Commissioning Intentions, etc.
   - The use of ICT and information assets and the responsibilities set out by law are unaffected by the categories below.
   - If yes please detail underneath in relevant section and provide priority rating and determine if full EIA is required.

		Positive Impact	Negative Impact	Reasons
Gender	Men			
	Women			
Race	Asian or Asian British People			
	Black or Black British People			
	Chinese people			

	People of Mixed Race			
	White people (including Irish people)			
	People with Physical Disabilities, Learning Disabilities or Mental Health Issues			
Sexual Orientation	Transgender			
	Lesbian, Gay men and bisexual			
Age	Children			
	Older People (60+)			
	Younger People (17 to 25 yrs)			
Faith Group				
Pregnancy & Maternity				
Equal Opportunities and/or improved relations				

Notes:

Faith groups cover a wide range of groupings, the most common of which are Buddhist, Christian, Hindus, Jews, Muslims and Sikhs. Consider faith categories individually and collectively when considering positive and negative impacts.

The categories used in the race section refer to those used in the 2001 Census. Consideration should be given to the specific communities within the broad categories such as Bangladeshi people and the needs of other communities that do not appear as separate categories in the Census, for example, Polish.

3 Level of Impact

If you have indicated that there is a negative impact, is that impact:			
		YES	**NO**
Legal (it is not discriminatory under anti-discriminatory law)		N/A	N/A
Intended		N/A	N/A

If the negative impact is possibly discriminatory and not intended and/or of high impact then please complete a thorough assessment after completing the rest of this form.

3.1 Could you minimise or remove any negative impact that is of low significance? Explain how below:	
3.2 Could you improve the strategy, function or policy positive impact? Explain how below:	
3.3 If there is no evidence that this strategy, function or policy promotes equality of opportunity or improves relations – could it be adapted so it does? How? If not why not?	
Scheduled for Full Impact Assessment	Date:
Name of persons/group completing the full assessment.	
Date Initial Screening completed	