University Hospitals Birmingham NHS Foundation Trust

CONTROLLED DOCUMENT

I.T. Acceptable Use Policy

CATEGORY:	Policy
CLASSIFICATION:	Governance
PURPOSE	The purpose of this policy is to provide a summary of the acceptable use that staff must be aware of when using various Trust information systems.
Controlled Document Number:	166
Version Number:	3.0
Controlled Document Sponsor:	Chief Medical Officer
Controlled Document Lead:	Head of IT Governance and Compliance
Will this Controlled Document impact upon any contracts held by the Trust?	☐ Yes[1] ☒ No
Approved By:	Board of Directors
On:	22/10/2020
Review Date:	22/10/2023
Distribution: • **Essential Reading for:** • **Information for:**	 All staff All staff

[1] If this Controlled Document will have an impact on any contracts held by the Trust, once approved, this will need to be sent to the Procurement Team requesting that it be added to the Procurement Policy Portal

Contents

Paragraph		Page
1	Policy Statement	3
2	Scope	3
3	Framework	4
	Email	5
	Internet	7
	Remote/mobile working	9
	Devices	10
	Passwords	11
	Software	12
	Copyright	12
	Equipment	12
	Printing/faxing	12
4	Duties	13
5	Implementation and Monitoring	15
6	References	15
7	Associated Policy and Procedural Documentation	16

Appendices

Appendix A	Glossary	18
Appendix B	Monitoring Matrix	21

1. Policy Statement

1.1 The purpose of this Policy and its associated documents is to outline the acceptable use, practices and responsibilities that are expected when University Hospitals Birmingham NHS Foundation Trust (the 'Trust') staff are provided with computer, storage, data and digital medical devices (including, but not limited to computer, tablet, smartphone) to conduct Trust business or interact with internal networks and business systems.

1.2 It is not the Trust's intention to impose restrictions to the Trust's established culture of openness, trust and integrity. However, the Trust is committed to protecting its staff from illegal or damaging actions by Trust staff, either knowingly or unknowingly.

1.3 Failure to comply with this Policy may result in disciplinary action being taken, which may result in dismissal or criminal prosecution.

1.4 The key objectives of this policy are to:

1.4.1 Set out a framework for Trust staff to follow to as a baseline for acceptable use of digital systems, services and equipment to enable the delivery of the best patient care and to help prevent adverse impacts on that care through inappropriate use.

1.4.2 Ensure all staff understand their roles and responsibilities in accordance with this acceptable use policy;

1.4.3 Define how monitoring and compliance with this policy will be assessed.

2. Scope

2.1 This Policy sets out the responsibilities for exercising good judgement regarding the appropriate use of information, all electronic devices and network resources to Trust staff where there is a defined business need in relation to IT applications, including but not limited to, the following:

2.1.1 Email

2.1.2 Internet

2.1.3 Remote/ mobile working

2.1.4 Devices

2.1.5 Passwords

2.1.6 Software

2.1.7 Copyright

2.1.8 Equipment

2.1.9 Printing/Faxing

2.2 This Policy applies to all areas and activities of the Trust and to all individuals employed by the Trust including contractors, volunteers, students, locum, bank and agency staff and staff employed on honorary contracts ('Trust Staff').

2.3 This Policy applies to all digital systems and services provided by or utilised by the Trust and all digital equipment used to access those services,

2.4 This Policy also applies to the use of @nhs.net addresses via the NHSMail system along with any other similarly externally provided services.

3. Framework

3.1 This Policy sets out the broad framework for the safe, efficient, and acceptable use of IT applications.

3.2 Under no circumstances are Trust staff authorised to engage in any activity that is could bring the Trust in to disrepute illegal while conducting Trust business, utilising Trust owned devices, network or email accounts. This includes, but is not limited to:

3.2.1 Introduction of malicious software or data into the network or server (e.g. viruses, worms, Trojan horses, email bombs, etc.).

3.2.2 Using a Trust computing asset to actively engage in procuring or transmitting material which is illegal.

3.2.3 Accessing data of which the member of Trust staff is not an intended recipient or logging into a computer or account that the member of Trust staff is not expressly authorised to access.

3.2.4 Execute any form of network monitoring which will intercept data not intended for the member of Trust staff, unless this activity is a part of their normal job/duty.

3.2.5 Introducing phishing scams to allow untrusted sites access to the Trust network.

3.2.6 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a member of Trust's staff's use of a device, via any means, locally or via the Internet/Intranet/Extranet.

3.3 In accordance with the Caldicott Principles, Person Identifiable Data (PID) must only be sent on a 'need to know' basis and there must be a justifiable reason to send this information.

Email

3.4 Email is not a confidential means of communication. The Trust cannot guarantee that electronic communications will remain private. Electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Once an email is transmitted it may be altered. Deleting or recalling an email will not eliminate it from the various systems across the Trust on which it has been transmitted. The burden of responsibility for the appropriate use of email lies with the sender of the message.

3.5 Trust email accounts must only be used for Trust business, save for the use of Trust email account for personal purposes which is permitted, provided this is not excessive, not in breach of Trust policies and does not interfere with the performance of a member of Trust staff's duties. The sending of personal emails must be marked accordingly in the Subject field.

3.6 The Trust SIRO has the final decision on deciding what constitutes inappropriate and/or excessive use.

3.7 All use of email must be consistent with Trust policies and procedures of ethical conduct, safety, compliance with applicable laws, and proper Trust practices.

3.8 All emails, whether work based or personal, are the property of the Trust, not the member of Trust staff. However, the individual Trust staff member and the Trust will be held jointly liable for communications containing statements about an individual, group or organisation that are proven to be offensive or in breach the duty of confidence.

3.9 Further guidance can be found within the associated Staff Code of Conduct.

3.10 Trust staff are prohibited from sending Spam emails. Please refer to the Trust's intranet on how to manage Spam received.

3.11 Trust staff must not send emails containing profanity and these messages may be blocked by the Trust's IT systems.

3.12 Email can be used as documentary evidence in disciplinary proceedings, harassment cases, complaints, libel and legal cases and

may be subject to Freedom of Information Act and Subject Access requests.

3.13 Save for the exceptions outlined below, the sending of PID via email is prohibited. Trust staff must check that all PID is removed from any emails or attachments before sending. Trust commercially confidential information must be treated with equal security considerations as PID.

3.14 Trust staff are restricted from using third-party email systems such as Google, Yahoo, and MSN Hotmail etc. to conduct Trust business, or to store or retain email on behalf of the Trust. Such communications must be conducted through Trust approved systems unless the Information Governance Group has approved an exemption.

3.15 The Trust email system users can exchange emails containing PID with other organisation that meet the NHS secure email standard. The Trust has implemented a secure collection portal for sending emails containing PID which are addressed to organisations that do not meet the NHS secure email standard. NHS mail provides an alternative secure email exchange system. For further guidance, please refer to the Trust intranet.

3.16 Trust staff must ensure that they know the email address of the person(s) they are sending a message to and obtain confirmation of receipt of important messages. This is particularly relevant where a message is being sent outside the Trust.

3.17 Staff are prohibited from automatically forwarding Trust email to a third party email system unless approved by the head of IT Governance/Compliance. Individual messages which are manually forwarded by the member of Trust staff to a third party email system, must not contain PID or Trust confidential information, unless there is a justified reason and the secure delivery method is used.

3.18 Trust staff must not send Email in a manner that deliberately attempts to bypass any system log-in or audit functionality or attempt to disguise themselves/their sending address in order to misrepresent any aspect of communication.

3.19 Emails, including mailshots, must only be sent to a person or group of people who have an interest in the subject. The use of ‘distribution lists’ must be treated with caution, particularly if PID information is included in the content. Third parties receiving an email may choose to treat it as a formal communication, as legally binding as if it had arrived on Trust headed paper. It is essential therefore that Trust staff do not make commitments in an email which exceed their authority or to enter into contracts outside the authority delegated to them by the Trust.

3.20 If Trust staff receive suspicious emails, these must be reported as spam and dispensed with. Under no circumstances must Trust staff undertake any further action in relation to suspicious emails (such as opening the email clicking on any embedded links, or attachments), except to report it to IT.. For detailed guidance, please refer to the Information Security and Access Control Policy and associated procedures.

3.21 The Trust reserves the right to suspend or remove access, temporarily or permanently, from any member of Trust staff suspected or convicted of misuse. Where a member of Trust staff is identified as potentially being in breach of this Policy, the Trust IT Services Department may be instructed to suspend the email account of that individual, pending further investigation and/or action.

Internet

3.22 The Trust recognises the benefits of the Internet, and electronic communications as valuable business communication tools, which must be used in a responsible, professional and lawful manner and in compliance with the Trust staff Code of Conduct. The Trust allows the use of these facilities provided patients and staff are protected from any adverse impacts caused by careless or inappropriate usage.

3.23 Undertaking illegal activities through the Trust's network is prohibited. Each Trust staff member accessing the network bears responsibility for, and consequences of, misuse of their access rights.

3.24 Trust material that is not already in the public domain must not be placed on any mailing list, public news group, or such service. If posting of such materials is necessary, it must be approved by the Communications Department.

3.25 The Trust's network must not be used for commercial activities unless this is specified within the Trust staff's role and responsibilities. This includes (but is not limited to) advertising, running any sort of private business.

3.26 Access to internet websites may be restricted as necessary by IT Services to ensure network and system security. IT Services may also limit access to content and in order to protect copyright. The Trust has the right to withdraw internet access from any member of Trust staff and globally ban access to any site without warning.

3.27 The Trust recognises that social media is a platform which will allow it to interact with stakeholders in order to enhance its profile, provide information about the role and aims of the organisation, make professional and developmental contacts, and to gauge and understand

the views of stakeholders such as patients. The Trust further recognises that social media platforms can benefit staff in building and maintaining professional relationships; establishing or accessing professional networks; seeking advice from forums; and accessing resources for professional development. However, Trust staff must ensure that confidentiality and the reputation of the business are protected at all times.

3.28 All staff must ensure that they remain vigilant of the difference between social and professional boundaries in IT system use by:

3.28.1 Not posting communication which may constitute threats of violence, bullying, intimidation or exploitation to other persons or property;

3.28.2 Not share confidential information inappropriately;

3.28.3 Not post pictures of patients, people receiving care, or staff;

3.28.4 Not post comments about patients;

3.28.5 Not use social media to build or pursue relationships with patients or service users;

3.28.6 Not use social media to defame or disparage the Trust staff or any third party; to harass, bully, stalk or unlawfully discriminate against staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties;

3.28.7 Not post communications which do not fall into the previous categories and which are reasonably considered as being grossly offensive, indecent or obscene;

3.28.8 Avoid making any social media communications which could damage the Trust's business interests or reputation, even indirectly;

3.28.9 Not express opinions on behalf of the Trust via social media, unless expressly authorised to do so by the Digital Communications Manager. Staff may be required to undergo training in order to obtain such authorisation;

3.28.10 Not post comments about sensitive business-related topics, such as Trust performance, or do anything to jeopardise the Trust's trade secrets, confidential information and intellectual property;

3.28.11 Not include the Trust logos or other trademarks, including photographs within which Trust premises are identifiable, in any social media posting or in their profile on any social media in a way that would bring the Trust into disrepute.

3.29 Personal use of social media is never permitted during working hours or by means of Trust computers, networks and other IT resources and communications systems. The only exception to this is if it is does so in accordance with the Trust's Social Media Procedure.

Remote/mobile working

3.30 Remote and mobile working are both methods which allow Trust staff to conduct Trust business whilst being off-site. Remote working is a method of accessing authorised network files and systems via a dedicated VPN connection, whilst mobile working includes any other work off-site. Trust staff undertaking remote and/or mobile working will be restricted to the minimum services and functions necessary to carry out their duties.

3.31 Trust staff must ensure that equipment, when used to conduct Trust business, will not be left unsecured at any time. Trust staff are responsible for ensuring that unauthorised individuals are not able to see information or access systems.

3.32 VPN tokens must be secured at all times and protected from unauthorised access. Any incident must be reported immediately to the IT service Desk and raised with the Risk and Compliance team in line with the Trust's Incident Reporting Policy/Procedure.

3.33 Use of any information or devices off-site must be for authorised work purposes only. Authorisation is to be obtained from the Trust staff member's line manager following a risk assessment.

3.34 If equipment is being used outside of its normal location and might be left unattended, the member of Trust staff is responsible for securing it by other appropriate means.

3.35 Save for any exception approved by the Senior Information Risk Owner (SIRO), all Trust IT portable equipment (i.e. a laptop, smart phone or tablet device) must be encrypted with Trust approved software before any information is stored. Where Trust staff have been supplied with such equipment they are responsible for ensuring that it is regularly connected to the Trust's network for upgrade of anti-virus software. Before equipment is returned, Trust staff must ensure any data is removed. Further guidance is provided within the associated IT Equipment Disposal Procedure. When Trust staff remove equipment,

files or data from Trust premises, they are responsible for ensuring its safe transport and storage.

3.36 Trust staff are only permitted to connect non-Trust acquired devices to the network via a secure method following consultation with IT Services and an approved risk assessment.

3.37 All confidential documentation, whether in paper or electronic format must be stored in a secure area when off-site, and stored securely during transit.

3.38 Timely incident reporting is crucial to minimise the risk of data loss. All lost or stolen devices must be reported to the IT Service Desk. Where possible, the Trust will employ remote wipe technology to remotely disable and delete any data stored when these devices are reported lost or stolen.

3.39 Devices required for remote and mobile working are provided to Trust staff subject to management approval. Where these are issued, family members or other acquaintances must not be permitted access to the equipment or data.

3.40 Any devices used for remote and mobile working must be connected via a secure network.

3.41 Whilst offsite if Trust staff decide to use any non-Trust devices for Trust business, under no circumstances must they save PID, confidential, or commercially sensitive information to these devices. Trust staff are responsible for ensuring that such devices have the relevant security configuration, including up to date anti-virus software.

Devices

3.42 Trust staff are responsible for their use of devices and connections and must take full responsibility for the security and protection of their devices and any information stored on the device. All assigned devices remain the property of the Trust and must be returned on termination of employment with the Trust or on the instruction of a manager. Returned devices will be wiped of any data by IT Services.

3.43 Patients and visitors may connect data devices to the Trust -guest Wi-Fi, where it is available and after accepting the terms and conditions.

3.44 Trust staff must not connect any non-Trust data devices to the Trust network or computers.

3.45 Staff must not use the SIM card provided to them with any device other than the one issued with the SIM card without prior approval from IT Services.

3.46 Only Trust-approved secure data devices or applications for example the Secure Clinical Image Transfer (SCIT) app must be used for the transfer of PID, confidential, or commercially sensitive data between computer systems when transfer via the Trust network is not possible. This data must not be transferred onto non-approved devices or networks. Data devices must not be used for data storage. Please refer to the Removable Media Procedure.

3.47 If travelling abroad for Trust business, staff must notify their line manager and IT Services prior to travel to ensure services will be available and that appropriate tariffs are in place.

Passwords

3.48 All systems and devices will be password protected to prevent unauthorised use. Passwords must comply with the complexity requirements as set out in the Access Control Procedure. Passwords must be changed on a regular basis or when prompted to do so.

3.49 Passwords and Smartcards must not be shared. The unauthorised access of passwords and/or smartcards must be reported immediately to the IT Service Desk and an incident must be raised with the Risk and Compliance team in line with the Trust's Incident Reporting Policy/Procedure.

3.50 If a member of Trust staff believes, or suspects, that another person is aware of their password, this must be changed immediately and IT Services informed. Trust staff must not attempt to remove or bypass the password protection.

3.51 Trust staff must not add additional password or security measures to any PC or files without first consulting with IT Services.

3.52 Trust staff must not leave any device unattended without activating password protections (either by logging out, activating a password protected screensaver or locking the device). Trust staff who discover an unattended device where a previous member of Trust staff has left their access open, must log out from the session or lock it before commencing their own session. Upon discovering an unattended and unlocked device, the member of Trust staff discovering the breach must follow the Procedure for the Reporting and Management of Incidents Including Serious Incidents Requiring Investigation.If the breach

involves PID; the Information Governance Department must be informed immediately.

3.53 Any actions undertaken using another Trust staff's user identity will be, in the first instance, presumed to be those of the account owner.

Software

3.54 Trust provided software is only for the purpose of conducting Trust business and bound by the vendors' license agreements. All business software on a device must either be provided and installed by IT Services or approved for download by the Trust. Under no circumstances must unapproved software be installed.

3.55 Trust staff must comply with any requests from IT to update software to ensure device security within 24 hours of receiving notification.

3.56 Any Trust staff being aware of, or suspecting, a security breach must immediately alert IT Services who will initiate investigative procedures.

Copyright

3.57 All staff must be aware of copyright protection when distributing articles or other third party original work by Email, or by posting it on the internet. This includes any form of digital media licensed solely for use by the Trust for Trust business.

Equipment

3.58 Only authorised Trust staff and third parties are permitted to move any ICT equipment, whether within an office or to another site unless approved by Head of Service Delivery.

3.59 Occasionally, suppliers may want to provide the Trust with free or new leased IT equipment. Staff must ensure they obtain appropriate authorisation first before accepting such offers and consult with IT Services. Further guidance can be found in the Trust's Hospitality, Gifts and Sponsorship Policy, the Staff code of Conduct and the Procurement Policy.

3.60 Trust staff must contact IT services if they wish to move or dispose of Trust IT equipment, including donated and leased equipment.

Printing/Faxing

3.61 Trust staff must only print/fax PID where absolutely necessary and with express approval by the SIRO. Staff must further take responsibility in

ensuring that faxed/printed information is collected from the equipment immediately and destroyed in line with Trust Policy.

3.62 For further information on how to fax information, please refer to the Trust's Safe Haven Procedure available on the intranet.

4. Duties

4.1 Chief Medical Officer

The Chief Medical Officer shall delegate approval of all procedural documents associated with this policy to the Director of IT services, and any amendments to such documents, and is responsible for ensuring that such documents are compliant with this policy.

4.2 Director of IT Services

The Director of IT has been delegated with responsibility for IT security on behalf of the Chief Executive. The day to day activities required to effectively implement and maintain this policy will be performed through the Head of IT Governance and Compliance.

4.3 Senior Information Risk Owner (SIRO)

The Director of Corporate Affairs is the Trust's SIRO and is accountable for fostering a culture for protecting and using data, providing a focal point for managing information risks and incidents, and is concerned with the management of all information assets.

4.4 Caldicott Guardian

The Trust's Caldicott Guardian role is fulfilled by the Trust's Deputy Chief Medical Officer has a strategic role in ensuring that there is an integrated approach to information governance, developing security and confidentiality policy and representing confidentiality requirements and issues at Board level.

4.5 Information Asset Owners

Information Asset Owners are senior individuals who are responsible for the risk management of their information assets. As such they have to understand what information is held, how it is used/transferred, who has access to it and why, in order for business to be transacted within an acceptable level of risk. They are therefore accountable for ensuring

that information assets have appropriate access controls in place and are used consistently and in line with the Trust Security and Access Control Policy.

4.6 Head of IT Governance and Compliance

The Trust's Head of IT Governance and Compliance is responsible for promoting a culture of good information security within the Trust and developing and maintaining policies, procedures and protocols in compliance with this policy and in accordance with good practice; along with joint responsibility for information security incidents with the Information Governance Lead. The Trust's Head of IT Governance and Compliance will be supported by the Lead Security and Test manager.

4.7 Information Governance Lead

4.7.1 The Senior Information Governance Manager is responsible for promoting a culture of good information governance within the Trust and developing and maintaining policies, procedures and protocols in compliance with this policy and strategy and in accordance with good practice.

4.7.2 In addition there exists an Information Governance Group which is chaired by the SIRO and comprises the Trust's Senior Information Governance Manager and IT Security and Test Manager. Through this group, common approaches are agreed to aspects of Information Governance and Security, where appropriate.

4.8 Digital Communications Manager

The Digital Communications Manager, on behalf of the Director of Communications and Executive Team, is responsible for granting authority for relevant staff to express opinions on behalf of the Trust via social media.

4.9 Managers

4.9.1 Anyone who has a responsibility for staff must ensure that:

a. They advise and inform their team of this policy to increase awareness and understanding;

b. They approve access to any Trust devices and software based on needs and after carrying out appropriate risk assessments;

c. They respond to any concerns raised in a timely fashion;

d. They maintain complete confidentiality relating to all aspects of investigations and do not mention or discuss such cases with any person not involved in it;

4.10 **Staff (including honorary contractors and volunteers)**

It is the responsibility of staff to ensure that they are using the services set out in this Policy in an appropriate way.

4.11 **Contractors**

4.11.1 In addition to the responsibilities for Trust staff, as detailed above, any contractor must obtain authorisation for use of their laptop, or alternative mobile device, on Trust premises. This must be obtained through the Trust manager they report to, who will co-ordinate the request with IT.

4.11.2 Any requirement to store Trust's data on a contractor's mobile device must have been specifically authorised by the information asset owner, and where necessary, if PID, confidential, or commercially sensitive information is stored then Information Governance approval is also required.

Any contractor's mobile device used to store Trust data will need to be encrypted to the Department of Health (DH) approved level, which can be verified with IT. Agreement on how PID, confidential or commercially sensitive is removed, and whether the device needs to be wiped, must be considered before any approval is granted.

5. Implementation and Monitoring

5.1 **Implementation**

This policy will be available on the Trust's Intranet Site. The policy will also be disseminated through the management structure within the Trust.

5.2 **Monitoring**

Appendix B provides full details on how the policy will be monitored by the Trust.

6. References

Caldicott Principles

Communications Act 2003

Computer Misuse Act 1990

Copyright, Designs and Patents Act 1988

Data Protection Act 2018

European Convention of Human Rights (Art 10. Right to freedom of expression)

Freedom of Information Act 2000
General Data Protection Regulation (EC 679/2016)

Malicious Communications Act 1988

Offences Against the Persons Act 1861

Protection from Harassment Act 1997

http://www.cla.co.uk/services/licences_available/nhs/NHS_england

https://www.gov.uk/government/publications/copyright-acts-and-related-laws

7. Associated Policy and Procedural Documentation

Access Control Procedure

Data Protection and Confidentiality Policy

Disciplinary Procedure

Emergency Preparedness Policy

Flexible Working Policy

Freedom of Information Act Policy

Information Governance and IT Security Incident Management Procedure

IT Equipment Disposal Procedure

Managing patients/public whose behaviour is inappropriate (Red and Yellow Card) Procedure

Mobile Devices Procedure

Prevention of Harassment and Bullying at Work Policy

Procedure for the Reporting and Management of Incidents Including Serious Incidents Requiring Investigation

Remote Working Procedure

Record Management (Corporate and Clinical) Policy

Safe Haven Procedure

Social Media Procedure

Staff Code of Conduct

Subject Access to Health Records Procedure

Violence & Aggression: Lone Worker Guidelines

Appendix A GLOSSARY

Anonymising Proxy allows the user to hide their web browsing activity. They are often used to bypass web security filters – e.g., to access blocked sites from a work computer**.**

Business Continuity is an organisation's ability to ensure operations and core business functions are not severely impacted upon by a natural disaster or other unplanned incident.

Business Critical Information Assets (BCIAs) are Information Assets which, if their confidentiality, availability or integrity were to be compromised or denied for a certain period of time, your organisation would cease to function. These Information Assets are directly owned by your organisation.

Cryptographic key means special data used in the process of encryption.

Devices Includes any device that can store data, images and other information required for the Trust's operational business. This includes laptops, tablets, personal digital assistants (PDAs), mobile, smartphones, phones, BlackBerry's, as well as digital audio and visual recording/playback devices (such as Dictaphones, digital cameras and mobile phones). Devices also include desktop computers.

DDOs Attack - Denial of service attack: this is where an attacker launches an attack against a system component and forces this component to limit or halt its normal service.

Digital Media Includes any physical items that can store data, images and other 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).

Encryption means the process of encoding a message or information in such a way that only authorised users can access it.

External Critical Information Asset are Information Assets which, if their confidentiality, availability or integrity were to be compromised or denied for a certain period of time, your organisation would cease to function. These Information Assets are not owned by your organisation; they are owned by external third parties but your organisation depends upon them for the delivery of critical services or in order to achieve business outcomes.

Extranet is an intranet that can be partially accessed by authorized outside users, enabling businesses to exchange information over the Internet in a secure way.

HSCN network - HSCN is a private network, designed as a reliable business resource to carry information, which is only available to certain organisations. This is different from a 'secure' network. It means that if patient data or personal data is being transmitted across HSCN, then encryption must be used.

HSCN agreement - The Connection Agreement sets out a collaborative way of working, which means:

- HSCN customers acknowledge responsibility for securing information - practically, this means that patient data should always be encrypted when being sent across any network, including the HSCN
- ownership and responsibility for the use of the HSCN connection sits at a senior level within the organisation

Information Asset Register is a register designed to aid organisations in understanding and managing their information assets in the fullest way possible, while also detailing the risks associated with them. This ensures that information can be protected and exploited.

Malware is a general term for malicious software. It is software that is designed to damage or perform unwanted action on a computer system. Malware includes viruses, worms, trojans and spyware.

Personal Identifiable Data (PID) is any information relating to an identified or identifiable Data Subject, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Personal Data – Special Category/ Sensitive refer to sensitive personal data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data; health data; sexual orientation or sex life.

Phishing refers to the process of deceiving recipients into sharing sensitive information with an unknown third party (e.g. a cyber criminal). It is a way of attempting to obtain data such as usernames, passwords, credit card information and other sensitive data. Attackers 'phish' (fish) for sensitive data through different methods.

Principle of Least Privilege means users are given the minimum access needed to perform their duty

Ransomware is software that denies you access to your files or computer until you pay a ransom; it is malicious software that can hold your data hostage.

Principle of Reasonable Use The test for reasonable use for this Policy will be determined by the Trust on a case-by-case basis.

Shared Drive Sharing a peripheral device (network folders, printer, etc.) among several users.

Social Media The term Social Media encompasses a variety of internet platforms (such as Twitter, Facebook, YouTube, Blogs and forums) which allow individuals and organisations to publish, and share information and comments online. It enables individuals to become part of different networks of people with similar interests.

Spam is irrelevant or unsolicited junk Email.

Spear-phishing is targeted phishing using spoof Emails to persuade people within an organisation to reveal sensitive information or credentials**.**

Stalking in the context of this policy it includes, but is not limited to contacting, or attempting to contact, another person by publishing a statement or other material on the internet which causes fear of violence, serious harm or distress.

VPN/ SSL VPN (virtual private network) is a method of connecting remote offices or computers to the central network. This method typically requires remote users to authenticate themselves by entering passwords or keys. A VPN allows users to communicate or access the organisation's servers securely over the internet.

Appendix B Acceptable Use – "Do's and Don't's"

The "Dos and Don'ts" of acceptable use of IT systems	Notes
Do keep your user names and passwords secret	
Do report anything suspicious to the IT service Desk	***We can all help the Trust be secure by being vigilant.***
Don't log on as anyone else.	
Don't use Trust systems for anything illegal	
Don't install software on Trust computers yourself	Event free software can often contain viruses etc.
Don't consider email, other than secure email safe	Email can be intercepted and PID stolen, unless secure
Do be courteous and professional in email	
Don't use your personal email for Trust business	
Do report Spam email if you receive it	***We can all help the Trust be secure by being vigilant.***
Do use the internet carefully and wisely	Just because a site may not be blocked, doesn't mean it's OK to use it!
Do look after the Trust equipment assigned to you	
Don't leave Trust IT equipment in risky places	
Do keep your devices up to date	Take any opportunity to accept device updates

Do take notice of copyright rules on software and data	
Do take care of any printed / faxed documents	
Do seek advice if you are unsure of anything, or something is suspicious	***We can all help the Trust be secure by being vigilant.***

Appendix C Monitoring Matrix

MONITORING OF IMPLEMENTATION	MONITORING LEAD	REPORTED TO PERSON/GROUP	MONITORING PROCESS	MONITORING FREQUENCY
Information Security and Access Control Management				
Information Security assurance.	Information Governance & Lead Security Manager	The Information Governance Group (IGG); final sign-off by the Board of Directors.	Information Security assurance is measured by the Trust's completion of the DSPT Data Security Protection Toolkit). The DSPT is an online system which allows NHS organisations to assess themselves against Department of Health Information Governance policies and standards.	DSPT submissions are required annually with interim assessments during the year, as determined by each new Toolkit release version.
Information security events and suspected near misses.	Lead Security Manager along with the appointed investigating officer.	All breaches will initially be reported to the Lead Security Manager for appropriate escalation and action; a summary of breaches is reported to the Information Governance Group. Serious incidents are included in the Trust's	All information security events and suspected near misses are to be identified and initially reported to the IT Service Desk, via the IT Service Centre Portal, for evaluation. Incidents and near misses must also be reported in line with the Trust's Reporting and Management of Incidents, Including Serious Incidents, Requiring Investigation Policy & Procedure. All breaches and incidents are then to be reviewed by the Trust's Information Governance Group and escalated as appropriate.	IGG meets quarterly; the Annual Governance Statement (AGS) and Annual Report are produced annually in line with internal cycle audit.

		Annual Governance Statement (AGS) and annual report, in line with HSCIC SIRI guidance.		
Reasonable use of Email (3.10)	Lead Security Manager	ISAG	Retrieval and reporting of the highest volume spam senders.	Quarterly
Offensive content sending (3.11)	Lead Security Manager	ISAG	Retrieval and reporting of the volume of email sent with potentially offensive content; along with content sampling.	Quarterly
Use of third-party email systems (3.15)	Lead Security Manager	ISAG	Retrieval and reporting of the highest volume users of external email systems (not NHSmail).	Quarterly
Appropriate use of internet resources (3.23)	Lead Security Manager	ISAG	Retrieval, summary reporting and sampling of the highest users of the internet connection and the most used sites	Quarterly
Mobile device policy compliance (3.36)	Lead Security Manager	ISAG	Retrieval, summary reporting and sampling of any mobile devices without encryption	Quarterly
Approved device connection (3.45)	Lead Security Manager	ISAG	Retrieval, summary reporting and sampling of devices making connection and blocking events	Quarterly
Password procedure compliance (3.49)	Lead Security Manager	ISAG	Retrieval, summary reporting and sampling of cases of poor password management compliance	Quarterly
Software management (3.55)	Lead Security Manager	ISAG	Retrieval, summary reporting and sampling of cases of software installations to expose any policy non-compliance	Quarterly
Incident Management				

Policy breaches	Information Governance Officer	Information Security Assurance Group	To report on any Information Security breaches in line with this policy	Quarterly
Implementation Compliance and Assurance				
This policy, along with associated documents, shall be subject to the Trust's internal audit process.	Internal Audit Team	Audit Committee	Where any shortfalls have been identified by the Internal Audit, these will be logged as recommendations to the senior management team, the completion of which is then monitored by the Audit Committee.	Annually