University Hospitals Birmingham NHS
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:	2
Controlled Document Sponsor:	Executive Medical Director
Controlled Document Lead:	Lead Security and Test Manager
Approved By:	Board of Directors
On:	October 2016
Review Date:	October 2019
Distribution: • **Essential Reading for:** • **Information for:**	 All staff All staff

Contents

Paragraph		Page
1	Policy Statement	4
2	Scope	4
3	Framework	5
	Email	6
	Internet	8
	Remote/mobile working	10
	Devices	11
	Passwords	12
	Software	13
	Copyright	13
	Equipment	14
	Printing/faxing	14
4	Duties	14
5	Implementation and Monitoring	17
6	References	17
7	Associated Policy and Procedural Documentation	18

Appendices

Appendix A	Monitoring Matrix	20

Abbreviations and Definitions

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.
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).
Person Identifiable Data (PID)	Any data which can identify an individual, including but not limited to forename, surname, address/postcode, telephone number, occupation, gender, date of birth, ethnic group, National Insurance number, NHS number, Trust reference number or any other information which will allow for the identification of the individual (e.g. rare event/disease).
Phishing	Phishing is the attempt to obtain sensitive information such as usernames and passwords details, often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.
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.
SPAM	SPAM is irrelevant or unsolicited junk email.
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.
Stalking	Stalking in the context of this policy 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	A Virtual Private Network (VPN) enables users to send and receive data across a shared or public network as if their computing devices were directly connected to the private network.

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 Hospital of Birmingham NHS Foundation Trust (the 'Trust') staff are provided with computer, storage, data and media 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 Executive Medical Director shall approve all procedural documents associated with this policy, and any amendments to such documents, and is responsible for ensuring that such documents are compliant with this policy.

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 and agency staff and staff employed on honorary contracts ('Trust Staff').

2.3 This Policy applies to all equipment that is owned or leased, by the Trust; and also any equipment that is either loaned or donated to the Trust.

2.4 This Policy also applies to the use of @nhs.net addresses, and NHSMail2 along with the NHSmail Acceptable Use Policy.

3. Framework

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

3.2 The Trust recognises the benefits of various technological advances to enable Trust staff to benefit its business objectives provided its reputation, patients and staff are protected from any adverse impacts caused by careless or inappropriate usage. This Policy provides a collection of measures for Trust staff to follow on the acceptable behavior in the use of these.

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

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

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

3.3.3 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.

3.3.4 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.

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

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

3.4 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

3.5 E-mail 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 e-mail is transmitted it may be altered. Deleting or recalling an e-mail from a Trust staff device 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 e-mail lies with the sender of the message.

3.6 Trust e-mail accounts must only be used for Trust business, save for the use of Trust e-mail account for personal purposes within reasonable limits which is permitted, provided this 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.

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

3.8 All use of e-mail must be consistent with Trust policies and procedures of ethical conduct, safety, compliance with applicable laws, and proper Trust practices.

3.9 All e-mails, 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:

- Defamatory
- Blasphemous
- Sexually or racially offensive
- Breach the duty of confidence

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

3.11 Trust staff must not send emails containing profanity as it is potentially offensive and these may be blocked by the Trust's IT systems.

3.12 E-mail 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 For further information regarding PID please refer to the associated Email Usage Procedure.

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

3.16 The Trust has implemented a secure collection portal for emails which contain PID. For further guidance, please refer to the Trust intranet. NHS mail and NHSMAIL2 provide an alternative secured send/receive system. Either of these must be used to send PID.

3.17 Trust staff must ensure that they know the e-mail 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.

3.18 Staff are prohibited from automatically forwarding Trust e-mail to a third party e-mail system. Individual messages which are manually forwarded by the member of Trust staff must not contain PID or Trust confidential information.

3.19 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.

3.20 E-mails, 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.

3.21 Third parties receiving an e-mail 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 e-mail which exceed their authority or to enter into contracts outside the authority delegated to them by the Trust.

3.22 If Trust staff receive suspicious e-mails, these must be deleted unless the recipient is able to verify with the sender that the email is genuine.

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, or forwarding it on).

3.23 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 e-mail account of that individual, pending further investigation and/or action.

Internet

3.24 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.

3.25 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.

3.26 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.

3.27 With the exception of Marketplace, 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, or fundraising for any charitable organisations not directly connected with the Trust.

3.28 Access to file downloads 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.

3.29 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.

3.30 All staff must ensure that they remain vigilant of the difference between social and professional boundaries by:

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

3.30.2 Not share confidential information inappropriately;

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

3.30.4 Not post inappropriate comments about patients;

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

3.30.6 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;

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

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

3.30.9 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;

3.30.10 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;

3.30.11 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.

3.31 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. Use of the Trust's own Marketplace site must be undertaken in accordance with the rules as set out in 'Marketplace' which is restricted to lunch breaks and other periods outside working hours.

Remote/mobile working

3.32 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.

3.33 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.

3.34 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.

3.35 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. Details as to the authorisation process are to be found in the associated 'Remote Working' procedure.

3.36 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.

3.37 Staff using mobile devices such as laptops are prevented from transferring confidential data as these do not have external device connectors installed.

3.38 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.

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

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

3.41 All Trust management incidents involving the use of remote working facilities must be reported in accordance with the Procedure for the Reporting and Management of Incidents Including Serious Incidents Requiring Investigation.

3.42 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.

3.43 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. Details as to the authorisation process are to be found in the associated 'Remote Working' procedure.

3.44 Any devices used for remote and mobile working must be connected via a secure network. Details are to be found within the Remote Working Procedure.

3.45 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.

<u>Devices</u>

3.46 Trust staff are responsible for their use of devices and connections and must take full responsibility for the security and protections 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.

3.47 Patients and visitors may connect data devices to the Trust QEHB Charity-guest Wi-Fi after accepting the terms and conditions.

3.48 Trust staff must not connect any non-Trust data devices to the Trust network or computers. The Trust does not permit Bring Your Own Device (BOYD).

3.49 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.

3.50 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.

3.51 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

3.52 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.

3.53 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.

3.54 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.

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

3.56 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.

3.57 Any actions undertaken using another Trust staff's user identity will be assumed to be those of the account owner.

Software

3.58 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.

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

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

Copyright

3.61 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 media licenced solely for use by the Trust for Trust business.

3.62 Copyright protection is afforded as soon as any of the following is created:

3.62.1 original literary, dramatic, musical and artistic work, including illustration and photography

3.62.2 original non-literary written work, e.g. software, web content and databases

3.62.3 sound and music recordings

3.62.4 film and television recordings

3.62.5 broadcasts

3.62.6 the layout of published editions of written, dramatic and musical works

Equipment

3.63 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 Gift/Hospitality and Sponsorship Policy, Staff code of Conduct and Procurement Policy.

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

Printing/Faxing

3.65 Trust staff must only print/fax PID where absolutely necessary. Staff must further take responsibility in ensuring that faxed/printed information is collected from the equipment immediately and destroyed in line with Trust Policy.

3.66 For further information on how to fax information, please refer to the Trust's Safe Haven Procedure available under the policy tab.

4. Duties

4.1 Director of IT Services

The Director of IT has been delegated with responsibility for information 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 Lead Security and Compliance Test Manager.

4.2 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.

4.3 Caldicott Guardian

The Trust's Executive Medical Director is the Caldicott Guardian and 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.

4.4 Director of Human Resources

The Director of Human Resources will arrange for suspected being breaches of this Policy and its associated documents to be investigated in accordance with the Disciplinary Policy and associated Procedure.

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 Policy.

4.6 Lead Security and Test Manager

The Trust's Lead Security and Test manager 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. The Trust's Lead Security and Test manager will be supported by the IT Security and Compliance manager.

4.7 Senior Manager Information Governance

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.

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 Compliance 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 IT Security and Compliance Manager

The IT Security and Compliance Manager is responsible for ensuring all returned mobile devices are wiped of data.

4.10 Managers

Anyone who has a responsibility for staff must ensure that:

- They advise and inform their team of this policy to increase awareness and understanding
- They approve access to any Trust devices and software based on needs and after carrying out appropriate risk assessments
- They respond to any concerns raised in a timely fashion
- 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

4.11 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.
All staff must:

- Protect their passwords;
- Ensure that all PID is removed from any emails or attachments before sending unless the exceptions are met;
- Ensure the use of e-mail is consistent with Trust policies and procedures of ethical conduct, safety, compliance with applicable laws, and proper Trust practices;
- Ensure that they know accurately the contact details of the person(s) they are sending message(s) to;
- Raise any concerns at the earliest possible opportunity, using Trust approved reporting channels;
- Maintain appropriate confidentiality during an investigation;
- Report any lost or stolen Trust devices immediately to the IT Service Desk
- Ensure adherence to the Trust's policy and associated procedure for the Reporting and Management of Incidents;
- Ensure that equipment is not left unsecured at any time;
- Make sure that remote equipment provided is regularly connected to the Trust network for relevant upgrades;
- Not connect any privately owned equipment to the Trust network unless prior approval has been given;
- Ensure their details are correctly maintained in the rDirectory;
- Comply with IT software update requests on receiving notification;

- Save Trust data on the Trust network (not their local hard drive);
- With the exception of nhs.net accounts, staff are prohibited from using third-party e-mail systems to conduct Trust business, or to store or retain e-mail on behalf of the Trust.
- Carry out a VDU assessment when working at home as set out in the associated Flexible Working Policy.

4.12 **Contractors**

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. Any requirement to store Trust's data on a contractor's mobile device must have been specifically authorised by the Trust's manager, and where appropriate, if PID, confidential, or commercially sensitive information is stored then Information Governance approval is also required; with the contractor's mobile device needing to be encrypted to the Department of Health (DH) approved level, this 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 A provides full details on how the policy will be monitored by the Trust.

6. References

Caldicott Principles

Communications Act 2003

Computer Misuse Act 1990

Data Protection Act 1998

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

Freedom of Information Act 2000

General Medical Council

Malicious Communications Act 1988

Nursing and Midwifery Council

Offences Against the Persons Act 1861

Protection from Harassment Act 1997

7. Associated Policy and Procedural Documentation

Access Control Procedure

Communicating Person Identifiable Data Procedure

Data Protection and Confidentiality Policy

Disciplinary Policy

Disciplinary Procedure

Email Usage Procedure

Flexible Working Policy

Freedom of Information Act Policy

Freedom of Information Act Procedure

IT Equipment Disposal Procedure

Information Governance Policy

Information Security Policy

Internet Usage Procedure

Marketplace Rules

Media Policy

Mobile Devices Procedure

Prevention of Harassment and Bullying at Work Policy

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

Record Management and Information Lifecycle Policy

Remote Working Procedure

Policy for the reporting and Management of Incidents including Serious Incidents Requiring Investigation

Staff Code of Conduct

Subject Access to Health Records Procedure

Violence & Aggression: Lone Worker Guidelines

Business Continuity Policy

Working Security Policy

Information Transfer

Appendix A Monitoring Matrix

MONITORING OF IMPLEMENTATION	MONITORING LEAD	REPORTED TO PERSON/GROUP	MONITORING PROCESS	MONITORING FREQUENCY
Information Security assurance.	Information Governance & Lead Security and Test 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 Information Governance Toolkit. The IG Toolkit is an online system which allows NHS organisations to assess themselves against Department of Health Information Governance policies and standards.	Toolkit 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 and Test Manager along with the appointed investigating officer.	All breaches will initially be reported to the IT 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 Annual Governance Statement (AGS) and	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 report, in line with HSCIC SIRI guidance.		
Policy breaches	Information Governance Officer	Information Security Access Group	To report on any Information Security breaches in line with this policy	Quarterly
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