Walsall Healthcare NHS
NHS Trust

Document Title
I.T. Acceptable Use Policy

Document Description	
Document Type	Trust Policy
Service Application	For all staff
Version	1.0

Lead Author(s)	
	Corporate Governance Manager
	Infrastructure Services Manager

Executive Director / Director / Manager

If you are assured that the correct procedure has been followed for the consultation of this policy, sign and date below:

Name	Director of Strategy and Improvement	Date	
Signature		01.04.2019	

Change History

Version	Date	Comments
0.1	01.11.2017	Initial draft
1.0	21.08.2018	Revised draft to meet National Data Standards/Toolkit requirements and link to disciplinary policy

Links with External Standards
Network & Information Systems Directive 2017
Data Protection Act 1998 General Data Protection Regulations 2017
Computer Misuse Act 1990
Investigatory Powers Act 2016
Data Retention & Investigatory Powers Act 2014
National Data Guardian for Health & Care Review of Data Security, Consent & Opt-Outs

Key Dates	DATE
Ratification Date	26th March 2019 by TMB
Review Date	September 2021

Executive Summary Sheet		
Document Title:	**I.T. Acceptable Use Policy**	
Key words:	**Access, Email, Information, Internet, IT Systems, Laptop**	
Please Tick (☑) as appropriate	This is a new document within the Trust	✓
	This is a revised Document within the Trust	
What is the purpose of this document?		
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.		
What key Issues does this document explore?		
The policy sets out the key responsibilities for exercising good judgement regarding the appropriate use of information, all electronic devices and network recourse to Trust staff where there is a defined business need in relation to IT applications, including but not limited to email, internet, remote/mobile working, devices, passwords, software, printing and copyright.		
Who is this document aimed at?		
All staff		
What other policies, guidance and directives should this document be read in conjunction with?		
IT Security policy NHS Digital Standards NHS Digital guidance for IT Systems in health & care settings RA Policy Disciplinary Policy Access Control Policy Safe Haven Policy Anti-Virus & Malware user guide Network & Information Systems Directive 2017 Information Sharing Policy Data Breach Policy & Procedure Confidentiality Policy Data Protection Policy & Procedures Data Protection Act 2018 General Data Protection Regulations 2017 Computer Misuse Act 1990 Data Retention & Investigatory Powers Act 2014 Media Policy		
How and when will this document be reviewed?		
The policy lead should review the document every three years or sooner if there is a change.		

CONTRIBUTION LIST

Key individuals involved in developing the document

Name	Designation
	Corporate Governance Manager
	Infrastructure Services Manager
	IT Business Manager
	Workforce Development & Information Systems Manager
	EUC Manager
	Service Desk Team Leader

Circulated to the following for consultation

Name / Committee / Group
Information Governance Steering Group
Policy & Procedures Group
Divisional Quality Teams
HR Sub Committee

Version Control Summary

Significant or Substantive Changes from Previous Version
A new version number will be allocated for every review even if the review brought about no changes. This will ensure that the process of reviewing the document has been tracked. The comments on changes should summarise the main areas/reasons for change.

When a document is reviewed the changes should use the tracking tool in order to clearly show areas of change for the consultation process.

Version	Date	Comments on Changes	Author
0.1	1/11/17	Initial draft	
1.0	21/8/18	Revised draft to meet national and toolkit requirements and link to legislation	

1.0 INTRODUCTION

1.1 The purpose of this policy and its associated documents is to outline the acceptable use, practices and responsibilities that are expected when Walsall Healthcare NHS 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.

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

1.2 Statement of Intent

This policy is based on existing good practice used in the NHS and sets out the principles and arrangements that must be adopted by all staff when accessing information systems.

1.3 Scope and limitations

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:

- Email
- Internet
- Remote/Mobile Working
- Devices
- Passwords
- Software
- Copyright
- Equipment
- Printing/Faxing

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').

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. It also applies to the use of @nhs.net addresses, an NHSmail.

2.0 POLICY AIM

The overall aim of the policy is to ensure Trust Staff operate within the parameters set for acceptable use.

3.0 OBJECTIVES

The policy sets out a framework for the safe, efficient and acceptable use of IT applications.

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 Staff to follow on the acceptable behaviour in the use of these.

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:

Introduction of malicious software or data into the network or service; i.e. viruses, worms, email bombs etc.

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

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.

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 duty.

Introducing phishing scams to allow untrusted sites access to the Trusts network.

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.

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

4.0 DEFINITIONS

Devices	Includes any device that can store images and other information required for the Trusts operational business; i.e. desktop computers. This includes laptops, tablets, personal digital assistants (PDAs), mobile phones/smartphones, as well as digital audio and visual recording/playback devices such as Dictaphones and digital cameras.
Media	Includes any physical items that can store data, images and other information and requires another device to access it. E.g. CD, DVD, disc, tape or portable hard drives, USB, memory cards.
Personal Identifiable Data (PID)	Any data which can identify an individual, including but not limited to name, address, telephone number, occupation, date of birth, ethnic group. National Insurance number, NHS number, hospital number or any other information which will allow for the identification of the individual.
Phishing	Phishing is the attempt to obtain sensitive information such as usernames and passwords, 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 folder, printer etc) among several users.
SPAM	Irrelevant or unsolicited junk email.
Social media	Internet platforms such as Twitter, Facebook, YouTube etc which allow individuals and organisations to publish and share information and comments online. It is enables individuals to become part of different networks of people with similar interests.
Virtual Private Network (VPN)	Enables users to send and receive data across a shared or public network as if their computing device where directly connected to the private network.

5.0 ROLES AND RESPONSIBILTIES

5.1 Associate Director of IT

The Associate 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 Infrastructure Services Manager.

5.2 Senior Information Risk Owner (SIRO)

The Director of Strategy and Transformation 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.

5.3 Caldicott Guardian

The Trust's 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.

5.4 Director of People & Culture

The Director of People & Culture will arrange for suspected breaches of this policy and its associated documents to be investigated in accordance with the Disciplinary Policy and associated procedures.

5.5 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 Trusts Information Security policy.

5.6 IT Infrastructure Services Manager

The Trust's IT Infrastructure Services Manager is responsible for promoting a culture of good IT 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 IT Infrastructure Services Manager will be supported by Associate Director of IT.

5.7 Corporate Governance Manager

The Trusts Corporate 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 the Information Governance Steering Group is in place to ensure common approaches are agreed to aspects of Information Governance and Security, where appropriate.

5.8 Digital Communications Manager

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

5.9 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 concerns raised in a timely manner;

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

5.10 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. They must:

- Protect their password;
- Ensure that all PID is removed from any emails or attachments before sending unless the exceptions are met;
- Ensure the use of email is consistent with Trust policy 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 opportunity, using Trust approved reporting channels;
- Maintain appropriate confidentiality during an investigation;
- Report any lost or stolen device immediately to the IT Service Desk;
- Ensure adherence to the Trusts policy and associated procedures for Reporting and Managing Incidents;
- Ensure that equipment is not left unsecured at any time;
- Make sure that the remote equipment provided is regularly connected to the Trust network for relevant updates;
- Not connect any privately owned equipment to the Trusts network unless prior approval has been given;
- Ensure their details are correctly maintained in the phone directory;
- 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 email systems to conduct Trust business, or to store or retain email on behalf of the Trust;

6.0 POLICY DETAIL

6.1 Email

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 recall an email from a Trust staff device will not eliminate it from the various systems across the Trust on which is has been transmitted. The burden of responsibility for the appropriate use of email lies with the sender of the message.

Trust email accounts must only be used for Trust business, save for the use of Trust email account for personal purposes within reasonable limits which is permitted, provided this does not interfere with the performance of a member of staffs duties. The sending of personal emails must be marked accordingly in the subject field.

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

All use of email must be consistent with Trust policies and procedures and in accordance with applicable laws and practice.

All emails, whether work based or personal, are the property of the Trust, not the member of Staff. However, the individual 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

Trust staff are prohibited from sending SPAM emails.

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

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.

Save for the exceptions outlined above, 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.

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

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 important where messages are sent outside the Trust.

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

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.

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 therefore essential 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.

If Trust staff receive suspicious emails, 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).

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 Trusts IT Services Department may be instructed to suspend the email account of that individual, pending further investigation and/or action.

6.2 Internet

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.

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

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.

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 staff and globally ban access to any site without warning.

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.

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

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

- Not share confidential information inappropriately;

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

- Not post inappropriate comments about patients;

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

- 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;

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

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

- 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.

- 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;

- 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.

Personal use of social media is never permitted during working hours or by means of Trust computer, networks and other IT resources and communication systems.

6.3 Remote/Mobile Working

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.

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.

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 Trusts Incident Reporting Policy and Procedure.

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.

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

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

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 Trusts network for upgrade of anti-virus software. Before equipment is returned Trust staff must ensure any data is removed.

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

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

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.

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.

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.

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

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.

6.4 Devices

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.

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

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

Only Trust approved secure data devices or applications 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.

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.

6.5 Passwords

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.

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 Trusts Incident Reporting Policy/Procedure.

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.

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

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 Reporting and Management of Incidents; including serious incidents requiring investigation. If the breach involves PID, the Information Governance Department must be informed immediately.

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

6.6 Software

Trust provided software is only for the purposes of conducting Trust business and bound by the vendor's licence 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.

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

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

6.7 Copyright

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.

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

- original literary, dramatic, musical and artistic work including illustration and photography;

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

- sound and music recordings;

- film and television recordings;

- broadcasts;

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

6.8 Equipment

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 Trusts policies and procedures.

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

6.9 Printing/Faxing

The Trust is taking steps to actively remove all faxes from use. For those that have no alternative, printing or faxing PID must only be undertaken as an absolute necessity. Staff must further take responsibility in ensuring that information is collected from the equipment immediately and destroyed in line with Trust policy.

For further information on how to send information securely please refer to the Trusts Safe Haven Policy available via the Intranet.

7.0 IMPACT ASSESSMENT

An equality impact assessment has been completed with regard to this policy and has not demonstrated any areas of impact or concern.

8.0 LINKS TO OTHER POLICIES

See Page 2 of this Policy.

9.0 LINKS TO EXTERNAL STANDARDS

See Page 2 of this Policy

10.0 MONITORING, CONTROL AND AUDIT

Monitoring Process	Requirements
Who	Corporate Governance Manager & IT Business Manager
Standards Monitored	Information security events and suspected near misses. Appropriate use of IT Systems and access.
When	Quarterly
How	Audits, Review and analysis of incidents
Presented to	Information Governance Steering Group & IOA
Monitored by	Information Governance Steering Group

Completion/Exception reported to	Quality & Safety Executive

11.0 BEST PRACTICE, EVIDENCE AND REFERENCES

Network & Information Systems Directive 2017
Data Protection Act 1998
General Data Protection Regulations 2017
Computer Misuse Act 1990
Investigatory Powers Act 2016
Data Retention & Investigatory Powers Act 2014
National Data Guardian for Health & Care
Review of Data Security, Consent & Opt-Outs
IT Security Policy
Safe Haven Policy
RA Policy
Information Security & Access Control Policy
Anti-Virus & Malware User Guides

Appendix 1: Acceptable Use – User Guide

General

Information technology resources, such as PCs, laptops, Smart Phones and Tablet devices offer new and exciting ways of working and engaging with our colleagues and patients. However, we must also be aware that improper use can impact us, our colleagues, patients, the reputation of the NHS and the public purse.
You will only be given access to systems and information that you require to carry out your work. Accessing or attempting to gain access to systems or information for which you have no 'Need to Know' or 'Need to Use', could be deemed a disciplinary offence.

In line with your organisational policies as well as legal and statutory requirements, you must always ensure that you adequately protect the confidentiality and integrity of any system or information you have been authorised access to. This includes protection against access by unauthorised persons.

Further guidance can be gained from your local Security Team and your Line Manager.

Protection of Systems

You should avoid eating or drinking in the vicinity of any IT equipment. Spilling drinks or food on to keyboards, monitors or other IT equipment could cause serious damage. You should avoid exposing IT equipment to anything that may damage or prevent normal operation, such as: sudden impacts, excessive change in temperatures or humidity.

Only authorised IT support personnel are allowed to open or move IT equipment or reconfigure or change system settings. You could cause serious damage if you attempt this yourself.

When left unattended, even for a short period, you should ensure that you lock your terminal/workstation/laptop/mobile device (using the Ctrl-Alt-Delete function or other applicable method). If left unattended in semi-controlled areas such as conference centres or customer offices or in the office overnight, laptops must be locked to a fixed point using a physical lock available from IT support.

You must ensure that you never leave portable equipment unattended in airport lounges, hotel lobbies and similar areas as these areas are insecure. Although it should be avoided, if you have to leave portable equipment in parked cars, you must ensure it is completely invisible from outside the vehicle and protected from extreme temperatures. When traveling by air, you must ensure that Portable equipment is carried as hand or cabin luggage at all times and not checked in to the hold.

If you are issued a Laptop or mobile devices it should only be used by you and not shared with or used by anyone else, including your work colleagues.

Do not connect privately owned or non NHS devices or use such devices with your NHS IT equipment or install unapproved or privately owned software on NHS IT equipment.

You must ensure that any device lost or stolen is reported immediately to your local Security Team.

Internet Acceptable Use

Internet access via the NHS infrastructure is provided for business purposes to simplify everyday tasks. Limited private use, such as access to web banking, public web services and phone web directories is accepted but excessive personal use of the Internet during working hours should be avoided.

You should not use NHS systems to access the Internet or use your NHS e-mail address for private business activities (such as eBay or auction sites), downloading software, images, music and videos or for personal financial advantage or for private social media and discussion forums.

Work Email Acceptable Use

Email services are provided to you for business purposes. Limited private use for the purpose of simplifying everyday tasks is accepted but private emails should be distributed via web based email services. Private emails should be stored in a separate folder named '*Private e-mail box*'. If retrieval of business emails is required (due to sick leave etc.) this folder will not be subject to inspection. Private emails should be deleted as soon as possible in order to limit storage requirements for non-business information.

You should not use external, web-based e-mail services (e.g. hotmail.com) for official or NHS business communications and purposes.

You must not distribute content that might be considered discriminatory, offensive, derogatory, abusive, indecent, pornographic or obscene, distribute statements of a political or religious or of a personal nature or engage in any illegal activities via e-mail.

Misuse of Information Systems

The use of NHS information or systems for malicious purposes or other than they were intended for could be deemed a disciplinary offence. This includes but is not limited to:

- Attempts to access external or internal systems you are not authorised for.
- Making discriminatory (on the grounds of sex, political, religious or sexual preferences or orientation), or derogatory remarks or accessing such material; this includes but is not limited to sending offending material as embedded or attached information in e-mails or other electronic communication systems.
- Acquiring or sending pornographic or material identified as offensive or criminal.

- Violating copyright or intellectual property rights, including use of obviously copyright-violated software.
- Accessing or attempting to access medical or confidential information without a legitimate purpose and prior authorisation.

Appendix 2: Checklist for the Review and Approval of Procedural Documents

To be completed and attached to any procedural document that requires ratification

	Title of document being reviewed:	Yes/No	Comments
1.	**Title**		
	Is the title clear and unambiguous? It should not start with the word policy.	Yes	Used NHSD template for this
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**		
	Are reasons for development of the document stated? This should be in the purpose section.	Yes	
3.	**Development Process**		
	Does the policy adhere to the Trust policy format?	Yes	
	Is the method described in brief? This should be in the introduction or purpose.	Yes	
	Are people involved in the development identified?	Yes	
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	There will be as per PPG/DQT process
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
	Are all terms clearly explained/defined?	Yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	N/A	
	Are key references cited?	Yes	
	Are the references cited in full?	No	UK legislation & WHT policies
	Are supporting documents referenced?	Yes	Listed in supporting documentation section

6.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
	If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?	Yes	Workforce Development & Information Systems Manager has seen initial draft
	For Trust wide policies has the appropriate Executive lead approved the policy?		
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	Yes	As per all Trust-wide policies
	Does the plan include the necessary training/support to ensure compliance?		
8.	**Document Control**		
	Does the document identify where it will be held?	Yes	
	Have archiving arrangements for superseded documents been addressed?	Yes	
9.	**Process to Monitor Compliance and Effectiveness**		
	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	Yes	
	Is there a plan to review or audit compliance with the document?	Yes	
10.	**Review Date**		
	Is the review date identified?	Yes	
	Is the frequency of review identified? If so is it acceptable?	Yes	
11.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the documentation?	Yes	

Reviewer			
If you are assured that the correct procedure has been followed for the consultation of this policy, sign and date it and forward to the Compliance and Risk Department for ratification.			
Name		Date	
Signature		Approving Committee/s	

Lead Manager (Local Policies) / Director (Trust Wide Policies)			
If you are assured that the correct procedure has been followed for the consultation of this policy, sign and date it and forward to the Compliance and Risk Department for ratification.			
Name		Date	
Signature		Approving Committee/s	
Ratification Committee Approval			
Quality Board minute number: PPG minute number: **TMB minute number:**			

Appendix 3: Equality Impact Analysis

Service Overview & Improvement Action Plan: Equality Analysis Form

Title: I.T. Acceptable Use Policy	What are the intended outcomes of this work? The policy sets out the key responsibilities for exercising good judgement regarding the appropriate use of information, all electronic devices and network recourse to Trust staff where there is a defined business need in relation to IT applications, including but not limited to email, internet, remote/mobile working, devices, passwords, software, printing and copyright.
Who will be affected? All staff	Evidence: N/A

ANALYSIS SUMMARY: considering the above evidence, please summarise the impact of the work based on the Public Sector equality duty outcomes against the 9 Protected characteristics			
Public Sector Duty *Protected Characteristics* (highlight as appropriate)	**Eliminate discrimination, harassment and victimisation**	**Advance equality of opportunity**	**Promote good relations between groups**
AGE / DISABILITY/ RACE	*No Impact*	*No Impact*	*No Impact*
SEX (Gender)/ GENDER REASSIGNMENT	*No Impact*	*No Impact*	*No Impact*
RELIGION or BELIEF/ SEXUAL ORIENTATION	*No Impact*	*No Impact*	*No Impact*
PREGNANCY & MATERNITY	*No Impact*	*No Impact*	*No Impact*

MARRIAGE & CIVIL PARTNERSHIP	*No impact*	*Not applicable at present*	*Not applicable at present*
What is the overall impact? There are no negative implications associated with this policy. The implementation promotes positive opportunities and relationships between all groups and is in accordance with the new General Data Protection Regulations.			
Any action required on the impact on equalities? *Impact of this policy has been assessed and it will not lead to any discrimination or other adverse events on any population groups, as described above.*			
Name of person completing analysis	*Corporate Governance Manager*	**Date completed**	*January 2019*
Name of responsible Director	*Director of Strategy and Improvement*		
Signature			