One + all | we care

Cornwall Partnership NHS
NHS Foundation Trust

NHS
Royal Cornwall Hospitals
NHS Trust

NHS
Kernow Clinical Commissioning Group

Acceptable Use Policy

V2.1

March 2020

Table of Contents

1. Introduction

1.1. This Policy is a requirement by NHS Digital and forms part of the evidence necessary to achieve compliance with the Data Security and Protection Toolkit. Toolkit compliance demonstrates the NHS's commitment to patient confidentiality and is a requirement to gain access to national NHS systems e.g. Health and Social Care Network (HSCN is the replacement for N3), NHS mail, Spine, eReferral (replacement for Choose & Book), etc.

1.2. This policy provides guidance on what is acceptable, as well as unacceptable, use of the organisations Information Communications Technology (ICT).

1.3. This policy covers the following areas of ICT:

- Responsibilities and use of Information Technology (IT) assets
- Use of e-mail and Internet
- Use of mobile devices, removable media and remote access
- Network usage (Including passwords/user access control)
- Use of patient information

1.4. This version supersedes any previous versions of this document.

1.5. Data Protection Act 2018 (DPA18) Legislation (General Data Protection Regulation – GDPR)

The Trust has a duty under the DPA18 to ensure that there is a valid legal basis to process personal and sensitive data. The legal basis for processing must be identified and documented before the processing begins. In many cases we may need consent; this must be explicit, informed and documented. We can't rely on Opt out, it must be Opt in.

DPA18 is applicable to all staff; this includes those working as contractors and providers of services.

For more information about your obligations under the DPA18 please see the 'information use framework policy', or contact the Information Governance Team (RCHT - rch-tr.infogov@nhs.net, CFT - cpn-tr.infogov@nhs.net, NHS Kernow -)

2. Purpose of this Policy/Procedure

The purpose of this policy is to protect patient information, Cornish Healthcare Organisations (CHO) and the NHS by ensuring that ICT equipment is used safely and appropriately.

3. Scope

3.1. This policy applies to all users of Cornwall ICT systems (namely staff and contractors associated with the organisations comprising of the Cornwall Health Organisations) and any other authorised user of the Cornwall NHS managed network.

3.2. It describes the responsibilities and acceptable use of ICT and Information assets hosted or accessed by Cornwall IT Services (CITS).

3.3. A failure to follow the requirements of the policy may result in investigation and management action being taken as considered appropriate. This may include formal action in line with the organisation's disciplinary or capability procedures for employees; and other action in relation to other workers, which may result in the termination of an assignment, placement, secondment or honorary arrangement.

3.4. Non-compliance may also lead to civil or criminal action being taken.

4. Definitions / Glossary

4.1. Applications/Software – Computer programs designed to store and manipulate information to support (or provide) a service.

4.2. Archive/Archived – Information that is no longer current which is retained to allow future access should the need arise. This may mean that the information is moved to slower access devices or compressed, but will still be accessible.

4.3. Availability – Ensuring that information is available at point of need for those authorised to access the information.

4.4. Backup – A copy (or the activity to produce a copy) of data stored on a computer. This is usually performed on servers and the copy of the data stored on a magnetic tape. This will enable the 'restoration' of information following a data loss incident and forms part of Business Continuity and Disaster Recovery activities.

4.5. Batch Processing – The manipulation/updating of information done after the event that initiated the change. Where changes cannot be implement at the time that they happen, they are stored and collected together to be updated at a later pre-determined time.

4.6. Blagging – See Social Engineering.

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

4.8. Business Continuity – The activity performed by an organisation to ensure that services are available to patients and staff. Business continuity will include a range of technical controls to maintain the availability of systems (based on it's criticality to the organisation) from identified 'threats' or vulnerabilities (such as loss of power, hardware failure, heat, etc.). Business continuity extends to delivering the service without access to IT services.

4.9. CITS – Cornwall IT Services, Royal Cornwall Hospitals Trust. CITS provide comprehensive Information and Communications support for the Cornwall Health Community and also varying levels of support to the wider Cornwall Health bodies (e.g. GP Practices, etc.). CITS online support portal can be accessed here: http://cits.cornwall.nhs.uk/ or you can call CITS Service Desk on extension 1717 (01209 881717). Non-urgent requests can be requested on the CITS Portal http://cits.cornwall.nhs.uk/.

4.10. Confidentiality – Ensuring that personal, sensitive and/or business critical information is appropriately protected from unauthorised access and is only accessed by those with an approved need to access that information.

4.11.Cornish Healthcare Organisations (CHO) – all organisations with a connection to the Cornwall COIN (including NHS Kernow (NHS K), Royal Cornwall Hospitals Trust (RCHT), Cornwall Partnership NHS Foundation Trust (CFT), GP's and other partner/commissioned organisations).

4.12.Cornwall COIN – a CITS managed community of interest network (COIN). This wide area network links all the computers across all Cornwall Health Organisations sites with the national HSCN network.

4.13.Critical Data Centre – Server room containing computers that process and store information relating to critical clinical and business systems.

4.14.Cyber Security – Is a term to cover defence against attacks primarily from the internet. These attacks can take many forms from direct hacking attempts, emails containing malware or links to infected websites, etc.

4.15.Critical Communications (Comms) Room – Network communication room (or cabinet) that is relied upon to provide access and availability to Cornwall Health Organisations critical clinical and business systems.

4.16.Database – an organised collection of information/data.

4.17.Disaster Recovery – The actions needed to restore systems/services following a break in service delivery outside of the agreed tolerance level. This is usually due to a major or unforeseen incident.

4.18.Encryption – The means of automating the protection of IT systems, information and data by making them unreadable without an electronic code from outside influences, e.g. computer viruses, unauthorised access to Cornwall Health Organisations hardware and software.

4.19.HSCN – Health and Social Care Network which replaced the National NHS Network (N3) transitioning from April 2017.

4.20.ICT – Information Communications Technology is the application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data and includes, but is not limited to:

- All network infrastructure including cables, wired and wireless access points.
- Network hardware including servers, storage and communications equipment.
- Personal hardware, i.e. desktop PC's & portable computers.
- Printers and Multi-function devices (MFDs)
- Peripheral equipment such as, keyboards, mice, digital pens and drawing tablets
- Software applications and systems, such as clinical and business systems whether hosted locally, on N3 or in the 'Cloud' (e.g. PAS, WebPACS, eReferals, RiO, etc.
- All generally installed software, such as NHS mail, Microsoft Office applications plus any additional software authorised for use by your organisation.

- Mobile IT devices such as Smartphone's, iPads including tablet PC, cameras and any other external device when connected either directly or wirelessly to the Cornwall Managed Network.
- All digital removable storage media e.g. Floppy disks, CDs/DVDs, memory sticks/flash drives, external hard disk drives and any other data storage device.

4.21. Integrity – Ensuring that information has not been corrupted, falsely altered or otherwise changed such that it can no longer be relied upon.

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

4.23. Memory Sticks – a portable (pocket sized) storage device used to transfer information between computers via the Universal Serial Bus (USB) port.

4.24. Mobile Device – These IT devices were designed to be able to provide PC functionality to support working whilst on the move or provide portable PC functionality which can be taken to different locations. Examples include laptops, tablets, Notebooks, PDA's, smart phones, etc.

4.25. N3 – The National NHS Network, a UK wide network connecting NHS organisations together (a private WAN). This has been replaced by the Health and Social Care Network (HSCN) which began to transition from April 2017.

4.26. Network – Connects IT equipment together to enable the transfer of information. Networks fall into one of these categories:

4.26.1. LAN – Local Area Network, joining computers and IT equipment in close proximity such as an office or building using wires.

4.26.2. WLAN – Wireless Local Area Network, the same as a LAN but using wireless technology (electronic signals/radio transmissions).

4.26.3. WAN – Wide Area Network, joining computers or other LANs across a large geographical area.

4.27. PC – Personal Computer a generic term used to describe most computers designed for use by one person at a time.

4.28. PID – Personal Identifiable Data/Information is information about a person which would enable that person's identity to be established by one means or another. This might be detail that would make it easy for someone to identify a person, such as an unusual surname or isolated Postcode or bits of different information which if taken together could allow the person to be identified. Person identifiable data includes one or more of the following;

- Name
- Postcode
- NHS Number or other identifiable number
- Date of Birth
- Clinical Diagnosis, where this is unusual or rare

4.29.Recovery – Restoration of a system to it's desired state following a failure in the operation of the system.

4.30.Remote Access – The ability to access information stored on the Cornwall NHS Network from a device not directly connected to it. This could be to support mobile working whilst not on Cornwall Health Community premises, home working or access by a third party organisation for the maintenance and support of a system/application. Remote access is via a number of approved, secure channels, but the preferred option is via Microsoft's Direct Access (this is automatically achieved when using a CITS provided laptop via an internet connection when not connected to the Cornwall Managed Network) or by Microsoft's F5 Big-IP through a secure portal which requires username, password and a generated key (e.g. from a 'Vasco' token) if not using CITS provided hardware.

4.31.Server – A computer on a network that runs one or more applications/ services (as a host) that can be accessed by other authorised users. This could be a database, file share, mail/printing services, etc.

4.32.Social Engineering (or Blagging) – Is where an attacker uses human interaction (social skills) to deceive others to obtain information about an organisation and its information assets including personal data. An attacker may potentially masquerade as a respectable and plausible person claiming bona fide interest in the information concerned e.g. posing as a member of the organisation's staff.

4.33.Social Media - A term commonly used for web-based and other mobile communications technologies that enable messages and opinions to be shared in dialogue with others.

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

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

4.36.Tweeting – See Blogging.

4.37.UPS – Uninterruptable Power Supply, a power supply that typically includes a battery to maintain power in the event of power outage. These can provide power for varying periods of time, but are primarily used within Cornwall COIN to provide protection from damage to servers from fluctuating power input and from short term power loss and resumption of power. The UPS is not for the purposes of business continuity as it will not provide power for a building.

4.38.User – Any person that accesses the Cornwall COIN. This includes, but is not limited to, non executive Directors, GP's, organisation employees, consultants, contractors, researchers, trainees, students and temporary staff.

5. Ownership and Responsibilities

5.1. Role of the Managers

Line managers are responsible for:

- Identifying the systems and levels of access that their staff need to be able to undertake their duties and seek authorisation for access from the appropriate Information Asset Owner (IAO).
- Completing and submitting the associated system access documentation to enable the account to be processed by Cornwall IT Services
- Annually reviewing your staff's systems access needs to ensure that it is still required.
- Ensuring that department/service information is transferred from personal network folders (such as the H:/ drive) to the appropriate shared folders when a member of staff leaves.
- Notify the Cornwall IT Services (CITS) Service Desk of any leavers or changes to staff roles so that access can be terminated or amended.
- Ensuring that their staff are aware and compliant with this Policy.

5.2. Role of the Information Governance Group

The Information Governance Group (RCHT)/Steering Group (CFT)/Sub Committee (NHS K) is responsible for:

- Reviewing the Policy
- Ratifying the Policy
- Publishing the Policy on the Document Library.
- Receiving reports highlighting risks and incidents relating to breaches of this policy.

5.3. Role of Cornwall IT Services (CITS)

CITS are responsible for:

- Maintaining the hardware and software components of the IT and communications infrastructure.
- Implementing all necessary technical and physical security controls to protect IT related Information Assets.
- Ensuring sufficient systems and processes are in place to monitor ICT activity to ensure compliance with IT policies, NHS standards and UK Law.
- Ensuring all new users accounts are created and accounts for those staff who have left are closed off in a timely manner.

5.4. Role of the Information Asset Owners

5.4.1. For the purposes of security, one local Information Asset Owner (IAO) will be appointed for each logical or physical set of information assets relating to software or applications. For shared systems, agreement will be reached on there being one owner. IAO's are responsible for:

- Understanding what information is held
- Knowing what is added and what is removed
- Understanding how information is moved
- Knowing who has access and why
- Approving 3rd party access to systems

5.4.2. These responsibilities are demonstrated by the following tasks:

- Ensuring that information assets receive an appropriate level of protection with regard to access to and handling of information.
- Ensure that a System Level Security Policy has been produced, detailing what the system does, the information stored and access and security controls in place to protect it. A review of staff who have access (and the level of access) should be undertaken annually.
- Ensure that a Data Protection Impact Assessment has been completed and is reviewed following any significant changes in the system that affects the information stored or access to the information.
- Business Continuity Plans have been documented and disseminated to staff to enable minimum services levels to continue in the event of a loss of IT services.
- Map the information flows both internally, with other systems, and externally to other organisations. Particular attention should be highlighted for any information flows outside the UK, these must be highlighted to the CITS IT Security Team and your Information Governance (IG) Lead.

5.5. Role of Individual Staff

5.5.1. IT systems are a business tool that should be treated like any other tool in the workplace. Staff and contractors should be aware that their line manager and colleagues may need to gain access to an individual's IT systems under certain circumstances (e.g. authorised need during absence). Staff and contractors are therefore advised to consider carefully the use of CHO provided IT systems for personal use.

5.5.2. All staff members are responsible for:

- Ensuring that that they have read and understood this Policy. Clarification as to what is Acceptable Use can be obtained from your Line Manager or CITS IT Security Team.
- Ensuring that any usage conforms to policy and legislation relating to IT security, confidentiality and data protection.
- Learning how to use IT systems and shared resources appropriately
- Filing copies of sent and received business emails in line with the Records Management: NHS Code of Practice.

6. Standards and Practice

6.1. Acceptable Use - General

6.1.1. Access to IT systems is primarily for business related purposes – to support (directly and indirectly) the provision of healthcare. Personal use of Email and the Internet is permitted provided this does not interfere with the performance of your duties or the duties of any other user in the Cornwall Heath Organisations. Personal access to IT systems can be limited or denied by your manager. Staff and contractors must act in accordance with organisational Policies and their manager's locally imposed restrictions.

6.1.2. Never leave your computer logged in whilst unattended, always logout or lock the screen before leaving, even if it is only briefly.

6.2. CHO User Names, Passwords and Smart Cards

6.2.1. Passwords are the first line of defence in protecting patient information and your account. They should be at least 8 characters in length and be a mixture of UPPER and lower case with numbers and/or special characters. They must not be easy to guess by someone who knows/researches you such as:

- Names of family members or pets
- Dates of birth
- Car registration numbers
- Telephone numbers
- Name of your favourite sports team
- Commonly used words relating to your area or specialty, such as Cornwall, Doctor, Maxims,
- A dictionary word with a number at the end (these are easy to crack by hackers who use tools to perform a 'dictionary' attack).

6.2.2. Be creative, try joining two different words together or using a letter sequence from the words of a favourite poem or saying.

6.2.3. Never repeat a password adding an incremental digit when requested to change password. E.g. United!1, United!2, United!3 etc.

6.2.4. Each user is responsible for maintaining the security of their individual login and password. Staff and contractors must not share their user name or password with anyone. If a breach of IT security is detected, the burden of proof will be with the user and owner of the password and login to show that they are not responsible for the breach. This includes staff and contractors that have remote access to the Internet. Never write passwords down, if you find it hard to remember your password, write a clue as an 'aide memoire'.

6.2.5. Never give you password to anyone else – there are no exceptions. If you feel your password may have been compromised, change it immediately and report it to the CITS Service Desk.

6.2.6. If you have forgotten your password, contact the CITS Service Desk who will be able to reset it. Repeatedly typing in the wrong password will block access for a period of time (so even if you do type in the correct password on

the tenth attempt – it will not be accepted). This is to prevent hackers using random key generators/programs from gaining login access.

6.2.7. Never write down password information or keep login details with any smartcard, laptop or USB memory stick. If it is stolen, or you lose it, you will be providing someone with everything they need to gain access.

6.2.8. Contractors who have secure, remote access to the Cornwall NHS managed network have additional responsibilities and must abide by the Third Party Supplier Remote Access Procedure.

6.2.9. Staff and contractors should log out when finished with IT systems. If a computer is found to be still logged in when you try to use it, you should always log the computer out and then login using your own account details. Any difficulties encountered whilst attempting this should be reported to the CITS Service Desk.

6.2.10. All users issued with a smart card are responsible for complying with the National Smartcard terms and conditions. Compliance will be monitored via line management arrangements, and Registration Authority Team audit. Any breach of these will be viewed as a disciplinary matter.

6.2.11. Never loan your smartcard to another person or disclose your PIN

6.2.12. Always remove your smartcard from the reader when not in use and keep it securely on your person.

6.3. Training

6.3.1. All staff are required to undertake annual Data Security Awareness Training (via the eLearning Portal in the NHS Electronic Staff Record (My ESR application)). This is an NHS mandatory requirement and compliance is reported via the Data Security and Protection Toolkit submission. Some training is delivered face to face which will be recorded as being of suitable content to attain compliance, this must be approved by the Learning and Development team. Induction does not count towards compliance as it does not have the required depth and range of topics.

6.3.2. Training must be successfully completed before access can be granted to certain medical systems. Training needs will be identified when your line manager requests access to a system via the CITS Service Desk/Portal.

6.4. Internet and Email

6.4.1. E-mail and Internet is now established as a major communication tool within the NHS. The CHO wish to encourage the correct and proper use and expects staff to use this facility professionally and ethically during their normal course of work.

6.4.2. This Policy and the Email Policy determines how users can use its e-mail and internet professionally, ethically and lawfully without compromising the security of the CHO systems and network and whilst maintaining patient/staff confidentiality. However, their use can expose the organisation to technical, commercial and legal risks if they are not used sensibly. It can also degrade the performance of the IT infrastructure due to excessive and inappropriate use.

6.4.3. The use of e-mail and internet is intended primarily for CHO business related purposes or professional development and training that supports the goals and objectives of the organisation.

6.4.4. Staff should therefore use this primarily for the legitimate business of the Trust and within the bounds of their authority

6.4.5. The aim of this policy is to:

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

6.4.6. This policy reflects the organisations strategy for access and usage of e-mails and the Internet.

6.4.7. **Permitted and prohibited Uses**

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

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

6.4.7.3. The Trust's may use automated content filtering software to restrict access to categories of websites that are deemed to be inappropriate, e.g. Adult/sexual, violence, criminal, etc. These are subject to on-going review. However just because you are able to access a particular website may not always mean that it is permitted.

6.4.7.4. The personal use of NHSmail is not discouraged provided this does not interfere with the performance of your duties, those of other staff members or the business of the Trust in general. Personal access to NHSmail can be limited or denied by your manager. Staff and contractors must act in accordance with Trust policies and their manager's locally imposed restriction. Personal emails should be stored in a folder marked 'personal'.

6.4.7.5. Do not use an email account that does not belong to you and do not allow others to use your email account.

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

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

6.4.7.8. Inappropriate or excessive personal use may result in disciplinary action and/or removal of e-mail facilities. Staff should be aware that both private and legitimate business use of e-mail will be subject to monitoring. There is no absolute right for staff to use the e-mail facilities for personal use You should only use the Trust's e-mail system for business use, subject to the rules in this policy.

6.4.8. **Offensive, Illegal and Defamatory Materials**

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

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

6.4.8.2. You must not under any circumstances use the e-mail system or Internet to access, download, send, receive or view any materials that you have reason to suspect are illegal.

6.4.9. **Social Networking and Blogging**

6.4.9.1. The use of blogging and social networking websites can expose the organisation to information risks, even where these sites are not accessed directly from work. The popularity of such websites and the rapid growth of internet enabled devices such Smartphones, iPads including Tablet PCs has resulted in significant awareness and uptake of these websites from home, from work and when mobile.

6.4.9.2. The risks that this may pose include:

- Unauthorised disclosure of business information and potential confidentiality breach.
- Legal liabilities from defamatory postings etc. by staff
- Reputational damage to the organisation
- Staff intimidation or harassment with possibility of personal threat or attack against the blogger, sometimes without apparent reason.
- Identity theft of personal data that may be posted
- Malicious code and viruses causing damage to IT infrastructure

6.4.9.3. Systems overload from heavy use of sites with implications of degraded services and non-productive activities, particularly in the use of rich media (such as video and audio) becoming the norm.

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

6.4.9.5. NHS organisations of all types are now making increased use of Social Networking facilities to engage their patients and other

stakeholders, to deliver key messages for good healthcare and patient service generally. These digital interactions are to be encouraged and their values extended as new communications channels become available for use.

6.4.9.6. Some CHO have embraced these patient engagement facilities and to ensure that the organisation is represented in a consistent way the organisations Communications Team will control the corporate social networking messaging, ensuring that it is utilised effectively and regularly monitored to remove any inappropriate content.

6.4.10. **Confidential and Sensitive Information**

6.4.10.1. Email and internet are not necessarily a secure way of sending information. NHSmail can be used to send highly confidential or sensitive information securely to another NHSmail account (i.e. @nhs.net to @nhs.net). Any other transmission of patient, confidential or business sensitive information must be encrypted to protect it whilst in transit.

6.4.10.2. Protecting information in transit can be achieved in a number of ways:

- Email encryption (NHSmail – enter '[secure]' in the email subject line).
- Encrypted USB stick.
- Secure File Transfer (sFTP) – contact the CITS Service Desk to access this facility.

6.4.11. **NHSmail (e-mail)**

6.4.11.1. NHSmail is the national e-mail and directory service developed specifically to meet British Medical Association requirements for clinical electronic messaging between NHS organisations and is the only NHS approved e-mail system for transmitting PID.

6.4.11.2. If you require a NHSmail account, contact the CITS Service Desk, so they can pre-register for this service.

6.4.11.3. All "NHSmail" e-mail addresses end in @nhs.net. All information sent between NHSmail accounts (i.e. both the sender and recipient) is protected in transit.

6.4.11.4. Emails containing patient identifiable or organisationally sensitive information that is sent to an address not on NHSmail MUST be encrypted. To encrypt an email, include '[secure]' in the subject line.

6.4.11.5. The 'message recall' function within NHSmail is not guaranteed and staff are advised to check the National NHSmail Directory to ensure they have the correct recipient before sending an email.

6.4.11.6. Do not include direct identifiers in the subject line, e.g. names, DoB, You can use Pseudonyms such as the CR or NNN.

6.4.11.7. Detailed information regarding the use of emails and NHSmail can be found in the Email Policy.

6.4.12. **Cyber Security (Malware, Viruses and Spam)**

6.4.12.1. All CHO managed computers and laptops have anti-virus software installed, which is regularly updated via the network.

6.4.12.2. The most common distribution method of all types of malware is by email. Malware can be hidden in email attachments (even pictures/images) or as a website link within the text of the email. To protect against threats, some types of files are automatically blocked by the email system (e.g. executable files (computer programs and games)) and documents and spreadsheets have 'macros' turned off by default (macros are embedded instructions within documents which can be abused to contain or download viruses and should never be enabled unless completely confident of the identity of the sender and you are expecting a document/spreadsheet which should contain macros).

6.4.12.3. Any emails that you believe may contain malware and viruses should be reported as phishing and then deleted immediately. If you have accidentally opened a suspicious attachment or clicked on a suspicious link, you must immediately report it to the CITS Service Desk as an incident so that it can be investigated and safely removed, as necessary.

6.4.12.4. Staff should examine carefully any email coming in to the organisation, including emails from known contacts as attackers can create authentic looking emails which 'pretend' to come from a legitimate source (this is known as 'spoofing').

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

6.4.13. **Housekeeping and Good Practice**

6.4.13.1. The following rules will help systems to work more efficiently:

- Messages should be reviewed and deleted on a regular basis and, if necessary, archived in accordance with the relevant organisations Policy to Manage Information and Records and the NHS Records Management: Code of Practice.
- Where possible, obtain confirmation from the recipient that an important e-mail has been received.

6.4.13.2. The amount of e-mail in the personal Inbox should be kept to a minimum and the inbox should not be used as a storage facility. Unless required for audit purposes, e-mails should be deleted after reading, response or action.

6.4.13.3. The e-mail system is designed for the transmission of messages and is not designed to be an archival system; staff should not rely on the e-mail system as a safe archive for important documents.

6.4.13.4. E-mails should be reviewed on a monthly basis and deleted when no longer required. The same housekeeping rules apply to 'Sent' Items.

6.4.14. **Email received in error**

Inform the sender if you receive a message sent to you in error. Delete the message from your mailbox. If an e-mail containing PID has been received in error, this must be entered on your Incident Reporting system (e.g. DATIX, Safeguard).

6.4.15. **Phishing email**

6.4.15.1. If you receive an e-mail with suspicious or fraudulent content do not respond to the email, open any attachments or click on any links. If you are using Outlook to read your messages, you can select the message in your 'Inbox' and click on the 'Report Phishing' button in the top left corner to report this to NHS Digital. Delete the email.

6.4.15.2. Advice can be sought from the CITS Service Desk.

6.4.16. **Email with warnings about criminal activity/frauds/scams**

6.4.16.1. Where there are genuine matters relating to security that staff need to be aware of these will be notified by the Police to CITS IT Security team or the local Counter Fraud specialists who in turn will issue warnings or guidance to staff.

6.4.16.2. If you receive e-mail purporting to give warnings about criminal activity or scams please do not forward these on to colleagues. Many of these are junk chain letters that have been circulating in one form or another for some time. Further advice can be sought from the CITS Service Desk

6.4.17. **Corporate Access (to cover a period of absence)**

6.4.17.1. For business continuity purposes it may be necessary for access to an individual's email account be given to a nominated manager of member of your team to cover a period of absence.

6.4.17.2. Ideally, this can be set up with your authorisation before a period of absence, but if there is an unexpected leave of absence, it may be necessary to provide access to your email so that important service requests can be facilitated.

6.4.17.3. NHSmail has a set of specific authorisation protocols which must be adhered to, before access can be granted (see Email Policy or the NHSmail website for more information).

6.4.18. **Legal Issues Relating to the use of Email and the Internet**

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

6.4.18.2. It is very important that you read this section to understand those issues as this will help you, and the Trust, to avoid problems.

6.4.18.3. These are not just theoretical issues. If the law is broken then this could lead civil and/or criminal liability for yourself and the Trust, as well as disciplinary action, including your dismissal. Ignorance of the law is not a defence in court

6.4.19. **Bullying and Harassment**

6.4.19.1. All employees are to be treated with dignity at work, free from harassment and bullying of any kind. It is strictly forbidden to send messages that contain offensive or harassing statements or language, particularly in respect of race, national origin, sex, sexual orientation, age, disability; religious or political beliefs. Remarks sent by e-mail that are capable of amounting to harassment may lead to complaints of discrimination under the Sex or Disability Discrimination Acts or the Race Relations Act. Bullying and harassment of any kind will be treated as a serious disciplinary matter which may lead to dismissal.

6.4.19.2. If you are subjected to or know about any harassment or bullying, whether it comes from inside or outside the organisation you are encouraged to contact your line manager, HR Advisor or Freedom to Speak Up representative immediately.

6.4.20. **Breach of Copyright**

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

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

6.4.20.3. E-mail users must observe all contractual, copyright issues. Under the Copyright, Designs and Patents Act 1988, copyright law can be infringed by making an electronic copy or making a 'transient' copy (which occurs when sending an e-mail). Copyright infringement is becoming more commonplace as people forward text, graphics, audio and video clips by e-mail. Employees must not copy; forward or otherwise disseminate third-party work without the appropriate consent.

6.4.21. **Formation of Contracts**

6.4.21.1. E-mail is capable of forming or varying a contract in just the same way as a written letter. Such capability gives rise to the danger of employees inadvertently forming contracts on behalf of the organisation or varying contractual terms to which the organisation then becomes bound.

6.4.21.2. For example sending an ambiguous e-mail to a contractor or supplier that could be misread as asking them to undertake some work on behalf of the Trust could be deemed a legal contract. Employees should take due care when drafting the words of an e-mail so that they cannot be construed as forming or varying a contract when this is not the intention.

6.4.22. **Defamation by Email or Internet**

6.4.22.1. The ease of use of e-mail can lead to unguarded comments being made, which in turn could be classified as defamatory. Defamation arises where there is the publication of an untrue statement tending to lower the subject of the statement (which may be an individual or an organisation) in the estimation of the public generally. Liability for the tort of defamation applies to electronic communication just as it does to more traditional forms of publishing.

6.4.22.2. Any expression of fact, intention and opinion via e-mail can be held against the author and/or the organisation, therefore do not include anything in an e-mail you are not prepared to account for or defend.

6.4.22.3. Employees are therefore advised to take care when drafting e-mails to ensure that they do not send messages that might be defamatory, incur liability on the part of the organisation or adversely impact on the image of the organisation.

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

6.4.23. **Obscene Materials**

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

6.4.24. **Protection of Personal Data**

6.4.24.1. The Trust is required to comply with the DPA/GDPR concerning the protection of personal data. Failure to adhere to that legislation could expose the Trust to civil liability and to enforcement action by the Information Commissioner Office (ICO)

6.4.24.2. Obligations under that legislation are complex but you can help ensure compliance by adhering to the following rules:

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

(NHS.net).

- Do not send any personal data outside the European Economic Area

6.4.25. **Freedom of Information (FOI)**

6.4.25.1. Although by its nature, e-mail seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of e-mail.

6.4.25.2. Under FOI legislation private email accounts used for business purposes are also subject to legislation, e.g. information contained in staff private email accounts can be disclosed if it is business related.

6.4.25.3. As defined in Records Management, e-mail is an electronic record. A printed copy of an e-mail is a hardcopy record. Information contained in an e-mail may be disclosed either in part or in whole to the public through the Freedom of Information Act (FOIA) or associated legislation. Although exemptions exist, staff and stakeholders need to be aware that the Trust cannot guarantee confidentiality of correspondence conducted by e-mail, as stated in the e-mail disclaimer.

6.5. Mobile/Remote Working

6.5.1. As Information and Communications Technology (ICT) has evolved over the years, it has changed the way many of us access and store information. Computer devices have been reducing in size, whilst communication facilities have been getting faster and more accessible in the workplace, homes and across the country. These elements have enabled many service areas to be able to work away from a traditional desk computer. Staff are not only able to move between computers within the organisation, many staff can move with their computers, within and outside their place of work. This has enabled clinicians to access patient information whilst on the wards, in the wider community, on the train, at home, etc.

6.5.2. Clinical applications are now being developed to embrace this mobile working philosophy and this will continue to transform the way we all work in the future. This new freedom not only changes the way that we work, but also ‘how’ we work. Information can become fragmented (stored in multiple places and not kept up to date) and it is also at greater risk of loss/unauthorised access.

6.5.3. **Mobile devices**

6.5.3.1. Examples of mobile devices include:

- Laptops, notebooks
- Tablets
- Smart phones

6.5.3.2. There are also a number of mobile storage media that are also enable mobile working by enabling the transfer of large amounts of information:

- Memory sticks
- Media players
- Removable/portable hard drives
- Optical discs (CD/DVDs)
- Tapes

6.5.4. **Security**

6.5.4.1. Physical Security – You are responsible for the physical security of the device. To protect against unauthorised disclosure of information and the loss/ theft of the device, you must:

- Always lock/shut down the device before leaving it.
- Ensure that the screen cannot be seen by others, be especially vigilant of who is around you when using mobile devices in public places.
- Return the device to the office environment and ensure it is securely stored if not in use for an extended period of time (e.g. on holiday).
- Hide the device from view if transporting in a car (preferably locked in the boot)
- Never leave it unattended in a non-secure or public place
- Report the loss or theft of any device immediately to CITS IT Service Desk, providing details of any sensitive data or PID stored on the mobile IT device.

6.5.4.2. Data Security – It is important that the data is protected from unauthorised access and that it's integrity is maintained (i.e. the information is accurate/up to date and accessible to authorised individuals who need to use it). There are a number of controls that must be applied to the device as well as actions that must be undertaken during it's use. These include:

- Encryption – It is mandatory for all NHS organisations to encrypt ALL mobile devices. All CITS provided mobile devices will be encrypted. You must not use an unencrypted mobile device or turn off encryption.
- Passwords – All of the security controls applied to the device are only as strong as your password. Once your password has been compromised, all information stored on the device, or accessible to you, will become available.
- Data integrity – Mobile working normally takes the form of 'Direct Access' or working on a copy of information. Direct Access creates a link back to the organisations servers and allows information to be updated within the live application/database, your shared network drives or your 'home' network drive (H:/). If you are not using Direct Access and you are working on a copy of the information or database (e.g. C:/ drive or 'My Documents') it is essential that this

information is transferred back to the organisations network/servers as soon as practicable. Information saved to mobile devices/storage is transitory, it is NOT backed up and the changes made will not be accessible to others within the organisation.

- Malware (Anti-Virus)

  CITS will ensure, as far as reasonably practical, that every device owned or explicitly approved for use by the CHO has an up-to-date installation of the necessary and appropriate anti-virus and security software, configured in line with current policies, procedures and best practice guidelines. CITS, in accordance with these policies, procedures and guidelines and, in line with any recommendations from the relevant suppliers, will undertake the regular updating of such software.

  CITS will also ensure that an up-to-date installation of the necessary and appropriately configured, anti-virus and security software is installed to protect e-mail and internet use in the CHO.

  Staff and contractors must take all reasonable steps to prevent the receipt and transmission of malicious software, e.g. computer viruses and in particular:

- Must not transmit any files which they know to be infected with a virus;
- Must not attempt to disable or remove the anti-virus and security software operating on any device owned, or explicitly approved for use, by the organisation;
- Must ensure that mobile devices are periodically connected to the network to ensure that the anti-virus and security software is kept up to date with the latest patches;
- Must ensure sufficient IT security measures are in place for home based computers used for secure, remote access to the Cornwall NHS managed network;
- Must not open electronic communications received from unsolicited or un-trusted sources

6.6. Use of Non CITS provided (personally owned) devices (BYOD)

6.6.1. BYOD (Bring Your Own Device) is a term used when staff use their own personal devices to undertake work duties. The use of personally owned devices is not permitted for any Cornwall Healthcare Organisation's duties, with the following exceptions:

- The use of personal phones to access NHSmail
- The use of personal/home computers to undertake non patient identifiable work (providing that the computer is appropriately licensed and protected).

6.6.2. Devices not provided by CITS should never be connected to the Cornwall NHS network without prior authorisation from the CITS IT Security Team.

6.7. Disposal of IT Assets

6.7.1. Staff must contact the CITS Service Desk to dispose of any IT Assets. Each organisation comprising of the CHO owns their PC's, Laptops and Servers. Disposals may be necessary as part of the agreed replacement programme, or for faulty equipment if it is deemed uneconomical to repair. It is only the organisation who owns the IT equipment which has the authority to decide whether their equipment is to be disposed and the responsibility of CITS to ensure that this is done securely (data destruction methods are based on media type as defined in the IT Security policy).

6.7.2. Disposal is the final chapter in the Asset Management Lifecycle and the importance of following strict, secure processes is often overlooked as the physical asset that has reached the end of its useful life and has limited financial value. However, it is likely to remain a significant information asset that, if not securely disposed, could result in an unauthorised disclosure breaching the Confidentiality: NHS Code of Practice, distress for the patient, a loss of public confidence in the NHS and a fine from the Information Commissioner's Office.

6.7.3. IT Technology allows for the storage of vast amounts of information which has traditionally been within dedicated server rooms. Due to technological advancements and the shift to a more mobile workforce, it is possible to store large amounts of business critical information on a number of portable and office related equipment (including laptops, memory sticks, cameras, multifunction printers, fax machines and photocopiers). It is important, therefore, to consider what happens to this equipment when it comes to the end of its life and leaves the CHO, to protect against an unauthorised disclosure incident.

6.7.4. It is important to note that information can be retrieved from any form of electronic storage (e.g. disks, memory sticks/cards, cameras, phones, backup tapes, etc.) after it has been deleted (and even after formatting the device). Therefore it is important that any device that has been used to store personal identifiable or sensitive organisational information is correctly sanitised before it is disposed of or passed on (this may include your own home PC if it is used for authorised work purposes).

6.7.5. Disposal of equipment may arise as follows:

- The IAO, in agreement with CITS, considers the equipment unsuitable for the required function
- The equipment is beyond economic repair
- Agreement by the Information Asset Owner, normally at the end of its useful life, for disposal under the capital replacement programme
- Agreement by the Policy Organisation for transfer to another body or organisation.
- The equipment is surplus to requirement and cannot be reused elsewhere within the CHO

6.7.6. In addition to Data Protection requirements, disposal of electronic equipment must comply with the Waste Electrical and Electronic Equipment

(WEEE) directive. If the IT equipment can be re-used, it will be redeployed elsewhere within the organisation which owns the equipment. Appropriate information security controls will be applied, based on risk and DHSC standards, as the device moves between security boundaries.

6.7.7. CITS are responsible for the secure disposal of items purchased by the CHO recorded on CITS IT asset register. The type of equipment that CITS are responsible for disposing includes:

- PC's
- Monitors
- Laptops, tablets and notebooks
- Printers
- PDA/Pocket PC's
- Electronic storage devices (e.g. memory sticks, CD/DVDs, floppy disks, etc.)
- Mobile Phones
- Keyboards and mice
- Docking Stations
- Backup tapes
- Servers
- UPS
- Switches and Hubs

6.7.8. CITS do not manage the disposal of the following types of devices:

- Medical Equipment (where patient information is entered)
- Photocopiers
- Fax Machines
- Monitor Stands
- Televisions
- DVD Players
- Video Recorders

6.7.8.1. Some of this equipment may retain information in memory (e.g. Photocopier and Fax machine) and specialist destruction will need to be sought - contact your line manager to arrange for secure disposal of this type of equipment.

6.8. New IT Systems

6.8.1. All new IT systems must be formally approved before purchase, whether they are purchased using departmental budgets or using external/charitable funding.

6.8.2. New systems requests must be submitted to the Chief Information Officer for submission to the appropriate Programme Board for authorisation. This is necessary to ensure that the system:

- Is compatible with current infrastructure
- Information Governance requirements (such as a Data Privacy Impact

Assessment) has been completed.

- Protects patient information.
- Has identified all the projects resources and costs and that appropriate resources are allocated to support implementation.

6.9. Unintentional Breaches of IT Security

If staff or contractors find themselves unintentionally viewing material, which may be inappropriate, they must make all reasonable attempts to close the application concerned immediately and inform the CITS Service Desk in line with the 'Procedure for Reporting IM&T Security Incidents'. A note of this unintentional access will be recorded and any content filtering rules modified where necessary to ensure that further unintentional access does not take place.

6.10. Download of Files

6.10.1. All file downloads should be automatically virus checked.

6.10.2. Audio, video and other file downloads must be in accordance with the laws which protect copyright, designs and patents.

6.11. Confidentiality

Staff and contractors are bound by the confidentiality, Data Protection, information governance and IT security policies of the organisation, by the common law duty to maintain confidentiality concerning the data and information used as part of their everyday work within the organisation, by legislation relating to data protection and the Records Management: NHS Code of Practice.

6.12. Periods of Absence

6.12.1. During planned periods of absence, such as holidays, please ensure that, where necessary, an appropriate work colleague has access to your documents and emails so that there is no disruption to service delivery.

6.12.2. During unplanned periods of absence, such as ill health, or where access has not been given to a work colleague, a line manager or Director may formally request that CITS provide access to a staff member's information, to minimise the disruption to service delivery. This must be authorised by the appropriate Director of HR/OD and Cadicott Guardian/Head of Information Governance and follow NHSmail requirements if access to NHSmail is required.

6.12.3. The most appropriate way to legitimately share information is by using shared drives and proxy email folders. These can be set up by contacting CITS Service Desk.

6.13. NHS Digital – Data Security and Protection Toolkit

CITS, acting on behalf of the CHO, are responsible for helping to maintain a safe and secure IT environment. More specifically, they are responsible for providing evidence to demonstrate that the organisation conforms to the elements of the Data Security and Protection Toolkit that relates specifically to IT security.

6.14. Monitoring Access

6.14.1. CITS may monitor any access on the Cornwall NHS managed network and any material accessed whilst remotely connected to the Internet which includes, but is not limited to, access to clinical (these audits should be undertaken by the Information Asset owner or suitable delegate) and non clinical applications, internet and e-mail access, audio, video and other file downloads, blogs, wikis, postings and instant messaging. The CITS IT Security Team is responsible for ensuring that audit tools are available which log the user, the material accessed, the time of day the material was accessed, the duration and if a file transfer took place.

6.14.2. These arrangements may include checking the contents of, and in some instances recording, the content of electronic communications for the purpose of:

- ascertaining or demonstrating standards which ought to be achieved by staff and contractors using the CHO IT systems;
- preventing or detecting crime;
- investigating or detecting unauthorised use of IT systems;
- ensuring effective operation of IT systems; or
- determining if electronic communications are relevant to the business - for example where an employee is off sick or on holiday
- assuring and protecting the reputation of the organisation

6.14.3. The organisation may, at its discretion, apply additional content monitoring and filtering systems as appropriate, and deny access to content that is unacceptable in the terms of this policy.

6.14.4. The organisation will make every reasonable attempt to prevent access to content likely to contain indecent, obscene or offensive material. This may on some occasions block content where legitimate access is required. Should staff or contractors find that they cannot access material which they have a legitimate need to access, they should contact the CITS Service Desk. The content filtering rules may be modified where necessary to ensure that further, legitimate access can occur.

6.14.5. These monitoring and control arrangements will operate on a continual and continuing basis, with the express aim of ensuring compliance with the provisions of the IT Security Policy.

6.15. Reporting on Use

6.15.1. The CITS IT Security Team will provide regular IT security incident and monitoring update reports. These reports will be made available to the organisation via the relevant Information Governance Group/Sub Committees.

6.15.2. If there appears to be excessive or inappropriate use of IT systems the CITS IT Security Team will be informed, who will raise the issue with the staff members senior manager or IG Lead as appropriate.

6.16. Breaches of IT Security

6.16.1. All major breaches in IT security or in the integrity of the network

and the associated connections will be reported to the IT Security Manager as soon as detected. The incident reporting procedure for the organisation concerned will be instigated immediately.

6.16.2. Incidents and outcomes of any investigations will be reported to the appropriate organisational Information Governance Group/Sub Committees.

6.17. Information Security Incident Reporting

6.17.1. An information security incident is defined as any event that has resulted or could result in:

- The disclosure of confidential information to any unauthorised person. This is unlawful under the Data Protection Act 2018.
- The integrity of the system or data being put at risk, such as identifying inaccurate or information that is not pertinent, finding ways around entering mandatory information, copying information to an insecure location.
- The availability of the system or information being put at risk. Damage done to computers or computer equipment (such as networks, back-up tapes etc.)
- An adverse impact e.g.
    - on reputation
    - threat to personal safety or privacy
    - legal obligation or penalty
    - financial loss
    - disruption of activities.

6.17.2. Some examples of these types of incidents include:

- Sharing of passwords, using someone else's id, password or pin number.
- Finding a computer printout of personal details in the street/car park.
- Finding a patient record in the back of an unattended wheelchair used by porters to move patients.
- Identifying that a fax that was thought to have been sent to a GP had been received by someone else.
- Losing a laptop or other mobile storage device (such as a USB memory stick, CD, DVD) with personal information on it.
- Giving out identifiable information about an individual over the telephone.
- Giving information to someone who should not have it – verbally, in writing or electronically.
- Accessing their own clinical records or those of family members, friends or notary individuals
- Accessing a prohibited website by accident.
- Sending a sensitive email to all staff by mistake.
- Finding an employees password written down on a 'post it'.
- Using another employees Smartcard or password to gain potentially unauthorised access to a system

- Finding someone has tried to break in to the office/building.

6.17.3. All incidents or information indicating a suspected or actual IM&T security breach will be reported to the immediate line manager and the CITS Service Desk.

6.17.4. The CITS Service Desk will provide a reliable, single point of contact for the receipt of notifications of IM&T security incidents. They will provide appropriate user or technical documentation and offer first line support to ensure that the risks relating to the reported IM&T security incidents are minimised.

6.17.5. The information to be reported:

- date of discovery of the incident
- place/location of the incident
- who discovered the incident
- details of the incident
- category/classification of the incident
- has the incident been reported to senior management if the incident puts the organization and/or patient care at risk?
- any action taken by the person discovering the incident.

6.17.6. The CITS IT Security Team are responsible for immediately notifying any IM&T security incident to the appropriate Information Governance Lead and the organisations Director responsible for information governance (herein known as the IG Team) as appropriate and, where necessary, gaining their explicit approval for investigation as necessary.

6.17.7. The CITS IT Security Team will risk assess the incident using both the Risk Classification Matrix and the Serious Untoward Incident (SUI) Matrix based on the information available and will record the incident on the CHO incident reporting system. Any IM&T security incident that scores three or higher on the SUI Matrix will be reported as an SUI in accordance with organisation procedures.

6.17.8. The CITS IT Security Team will record the incident on the organisation Incident Reporting System (if accessible) and on the CITS IT Security Risk Register.

6.17.9. The CITS IT Security Team will relate incidents with similar characteristics thereby helping them to respond to any areas of vulnerability or to identify any area where greater user awareness is needed.

6.17.10. Once explicit approval has been obtained to undertake any investigation (where necessary) the CITS IT Security Team will:

- provide the staff member with details of the planned investigation
- inform other key teams or staff members both within the CHO and CITS
- inform the Local Security Management Specialist (LSMS) and the Local Counter Fraud Specialist (LCFS) where appropriate
- investigate, collate and record all information pertaining to the incident in line with the organisation’s Incident Reporting and Investigation Policy

- prepare an interim report and submit this to the IG Team, the LSMS, the LCFS and/or the reporting staff member as appropriate
- prepare a summary report of the incident, the risks identified and any recommendations and action plans identified for presentation to the organisation's Information Governance Committee/Sub Committee
- liaise with the CITS Management Team, the IG Team, the LSMS, the LCFS and the reporting staff member as appropriate to ensure that recommendations and action plans identified as a result of any investigation are implemented and regularly monitored.

6.17.11. Some incidents may involve the invoking of Disciplinary and Capability Procedures.

6.17.12. Incidents should be used in training sessions about security and confidentiality as using 'real life events' relating to an organization can always be related to, by staff, better than to imaginary events. This will give attendees an example of what could occur, how to respond and how to avoid such events in the future.

6.18. Action in the Event of a Breach of Policy

6.18.1. In certain circumstances where there is assessed to be a risk to networks, IT systems or data CITS will, as a first action, act promptly to prevent continuance or repetition of the breach. This action will be taken in accordance with the organisation's policy and procedures and incident reporting procedures involving liaison between CITS, the organisation's Senior Information Risk Owner, Corporate Risk Manager, Information Governance Manager, Human Resources, the Local Security Management Specialist, the Local Counter Fraud Specialist or the Health Records Manager.

6.18.2. Indications of non-compliance with the provisions of this policy will be investigated, as appropriate, in accordance with disciplinary procedures. Where necessary line management, Human Resources and other departments and external organisations, such as the Child Protection Team and the Police, will be involved.

6.18.3. Subject to the findings of any such investigation, non-compliance with the provisions of this policy may result in disciplinary action being taken, which may result in dismissal or criminal prosecution.

6.19. Disclaimers

The organisation will supply an appropriate disclaimer that should be appended to all electronic communications that are sent externally.

7. Dissemination and Implementation

7.1. The Acceptable Use Policy should be made available and referenced as part of staff induction.

7.2. Line managers have a responsibility to ensure that their staff, that use ICT, understand and comply with the Acceptable Use Policy.

7.3. The Acceptable Use Policy will be published on the Intranet or a paper copy can be requested from the CITS Service Desk.

8. Monitoring compliance and effectiveness

Element to be monitored	This policy will be monitored to ensure that the CHO are compliant with the NHS Digital Data Security and Protection Toolkit.
Lead	CITS IT Security Team
Tool	Software tools will be used where appropriate to monitor activity and compliance with this policy which will be periodically reviewed and will be made available in the course of an IT security investigation.
Frequency	Acceptable Use is enforced by the implementation of security controls and is monitored on a daily basis.
Reporting arrangements	Incidents or breaches of this policy are reported to the Head of Information Governance, which may also be reported to the Information Governance Group/Sub Committees or SIRO depending on their seriousness.
Acting on recommendations and Lead(s)	Recommendations will be made by the Clinical Informatics Development Plan Board, Information Governance Group (Sub Committee), CITS IT Security Team and National best practice. Implementation action plans will be agreed by the organisation's IGG/IGSC, Clinical Informatics Development Plan Board and updates reports will be provided as appropriate.
Change in practice and lessons to be shared	Any lessons learnt during the reviews and audits will inform and update the Acceptable Use Policy which will be presented to the appropriate IGG/IGSC for consultation and ratification.

9. Updating and Review

9.1. This Policy will be reviewed no later than every three years.

9.2. Revisions can be made ahead of the review date when the procedural document requires updating. Where the revisions are significant and the overall policy is changed, the CITS IT Security Team will re-submit the Policy to the organisations IGG/IGSC for consultation, ratification and dissemination.

9.3. Any revision activity is to be recorded in the version control table as part of the document control process.

10. Equality and Diversity

10.1. This document complies with the Royal Cornwall Hospitals NHS Trust service Equality and Diversity statement which can be found in the 'Equality, Inclusion & Human Rights Policy' or the Equality and Diversity website.

10.2. Equality Impact Assessment

The Initial Equality Impact Assessment Screening Form is at Appendix 2.

Appendix 1. Governance Information

Document Title	Acceptable Use Policy V2.1			
Date Issued/Approved:	February 2020			
Date Valid From:	March 2020			
Date Valid To:	25th March 2022			
Directorate / Department responsible (author/owner):	Andrew Mann, IT Security Manager			
Contact details:	01209 318647			
Brief summary of contents	This Policy describes what behaviour is acceptable and unacceptable when using Information Communication Technology equipment on behalf of an organisation that is a member of the Cornwall Health Community.			
Suggested Keywords:	Acceptable Use, IT Use, IT User, IT Policy, Computer.			
Target Audience	RCHT	CFT	KCCG	
	✓	✓	✓	
Executive Director responsible for Policy:	Director of Strategy and Business Development			
Date revised:	23/11/18			
This document replaces (exact title of previous version):	Acceptable Use Policy V2.0			
Approval route (names of committees)/consultation:	Information Governance Group (RCHT), Information Governance Sub Committee (CFT, NHS Kernow)			
Divisional Manager confirming approval processes/organisation	Kelvyn Hipperson			
Name and Post Title of additional signatories	Not Required.			
Signature of Executive Director giving approval	{Original Copy Signed}			
Publication Location (refer to Policy on Policies – Approvals and Ratification):	Internet & Intranet	✓	Intranet Only	
Document Library Folder/Sub Folder	Health Informatics/ Infrastructure/Technical/Security			
Links to key external standards	Records Management: NHS Code of Practice Confidentiality: NHS Code of Practice The Data Protection Act 2018			

	HMG Security Policy NHS Digital Data Security and Protection Toolkit The Health and Safety at Work Act 1974 Companies Act 1985 Copyright, Designs and Patents Act 1988 Computer Misuse Act 1990 Human Rights Act 1998 Regulation and Investigatory Powers Act 2000 Freedom of Information Act 2000 Health and Social Care Act 2000 Electronic Communications Act 2000 Private Security Industry Act 2001 Copyright and Related Rights Regulations 2003 Police and Justice Act 2006 Fraud Act 2006
Related Documents:	The IT Security Policy Policy for the safe disposal of IM&T equipment and electronic media Email Policy Policy for managing health records Policy for Recordings and Photography Disciplinary Policy Equality and Diversity policies Fraud and Corruption Policy/Counter Fraud and Corruption Policy
Training Need Identified?	Yes - Induction

Version Control Table

Date	Version No	Summary of Changes	Changes Made by *(Name and Job Title)*
24/03/10	V1.0	Reformatted - Adopted IGM	Andrew Mann, IT Security Manager
20/08/10	V1.1	PCT changes accepted (Corporate Gov)	Andrew Mann, IT Security Manager
05/05/11	V1.2	PCT IGSC changes in line with IGT v8 guidance /requirements	Andrew Mann, IT Security Manager
14/09/11	V1.3	Added references to supporting Policies/ Acts following PCT Counter Fraud review	Andrew Mann, IT Security Manager
25/02/14	V1.4	Updated to RCHT's Policy template format	Andrew Mann, IT Security Manager
21/08/15	V1.5	Updated wording to be applicable across the Cornwall Health Community	Andrew Mann, IT Security Manager
20/03/17	V1.6	Expanded information relating to use of Internet and email. Added information relating to Cyber Security.	Andrew Mann, IT Security Manager

24/04/17	V1.7	Added information regarding the disposal of IT assets and some minor changes following the CFT consultation.	Andrew Mann, IT Security Manager
23/11/18	V2.0	Government Secure Network email addresses are no longer considered protected in transit. Encryption for emails containing patient information no required. Updated to reflect DPA18 and Data Security and Protection Toolkit. Added information relating to New IT Systems and BYOD.	Andrew Mann, IT Security Manager
01/03/2020	V2.1	Changes made to reflect new requirements in the Data Security and Protection Toolkit, including improved password advice to users.	Andrew Mann, IT Security Manager

All or part of this document can be released under the Freedom of Information Act 2000

This document is to be retained for 10 years from the date of expiry.

This document is only valid on the day of printing

Controlled Document

This document has been created following the Royal Cornwall Hospitals NHS Trust Policy on Document Production. It should not be altered in any way without the express permission of the author or their Line Manager.

Appendix 2. Initial Equality Impact Assessment Form

Name of the strategy / policy /proposal / service function to be assessed **Acceptable Use Policy V2.1**					
Directorate and service area: Cornwall IT Services			**Is this a new or existing Policy:** Existing		
Name of individual completing assessment: Andrew Mann			**Telephone:** 01209 318647		
1. *Policy* Aim* *Who is the strategy / policy / proposal / service function aimed at?*	This Policy describes what behaviour is acceptable and unacceptable to all users of Information Communication Technology equipment on behalf of an organisation that is a member of the Cornwall Health Community.				
2. *Policy* Objectives*	To define the behaviour that is expected when using Cornwall Health Communities ICT facilities to protect patient and organisational information and the reputation of the organisation and NHS.				
3. *Policy* – intended Outcomes*	To inform Cornwall Health Community users of acceptable and unacceptable behaviour whilst using Information Technology whilst undertaking their duties.				
4. *How will you measure the outcome?	By reviewing the number of breaches/incidents reported.				
5. Who is intended to benefit from the *policy*?	Users of the Cornwall Health Community ICT infrastructure and devices.				
6a Who did you consult with	Workforce	Patients	Local groups	External organisations	Other
	X		X		
b). Please identify the groups who have been consulted about this procedure.	**Please record specific names of groups** Cornwall Health Community, Information Governance Group/Sub Committee.				
What was the outcome of the consultation?	Approved				

7. The Impact
Please complete the following table. **If you are unsure/don't know if there is a negative impact you need to repeat the consultation step**.

Are there concerns that the policy **could** have differential impact on:				
Equality Strands:	Yes	No	Unsure	Rationale for Assessment / Existing Evidence

Age		✓		
Sex (male, female, trans-gender / gender reassignment)		✓		
Race / Ethnic communities /groups		✓		
Disability - Learning disability, physical impairment, sensory impairment, mental health conditions and some long term health conditions.		✓		
Religion / other beliefs		✓		
Marriage and Civil partnership		✓		
Pregnancy and maternity		✓		
Sexual Orientation, Bisexual, Gay, heterosexual, Lesbian		✓		

You will need to continue to a full Equality Impact Assessment if the following have been highlighted:

- You have ticked "Yes" in any column above and
- No consultation or evidence of there being consultation- this excludes any *policies* which have been identified as not requiring consultation**. or**
- Major this relates to service redesign or development

8. Please indicate if a full equality analysis is recommended.	**Yes**		**No**	✓

9. If you are **not** recommending a Full Impact assessment please explain why.

The Policy give guidance on what the Trust deems acceptable and unacceptable behaviour based on NHS standards and general best practice.

Date of completion and submission	February 2020	Members approving screening assessment	Policy Review Group (PRG) **APPROVED**

This EIA will not be uploaded to the Trust website without the approval of the Policy Review Group.

A summary of the results will be published on the Trust's web site.