echogenicity

September 2019

www.echogenicity.co.uk

Acceptable Use Policy

Scanning Cornwall's Hearts

Table of Contents

1. Introduction

1.1. Echogencity Staff and contractors of the Cornwall Health Community (CHC), are provided with access to Information & Technology (IT) systems. It is therefore essential that policies and procedures are in place to manage and control access including:

Guidance to each user as to acceptable and unacceptable use including:

- Defining what is acceptable use, including what is acceptable personal use;
- Defining what is unacceptable use, including personal use during working time and accessing of indecent, obscene or offensive material;
- Defining the consequence of unacceptable use;

Ensuring that each user is aware of this policy and has confirmed their understanding and acceptance of the policy;

Putting in place mechanisms to monitor users and their usage;

Putting in place mechanisms that prevent access to indecent, obscene or offensive material;

Ensuring that breaches of this policy are dealt with quickly and in line with disciplinary procedures where necessary that involve Verity Williams Curnow MD and external organisations, such as the Child Protection Team and the Police, where appropriate and necessary;

Ensuring that identified Serious Untoward Incidents (SUIs) are reported

To Verity Williams Curnow in accordance with policy.

Ensuring that identified Critical Incidents (CIs) are reported to Verity Williams Curnow accordance with policy.

1.2. The underlying philosophy is that the CHC IT systems should be used in a manner which is ethical, legal and appropriate to the CHC aims. The CHC encourage the use and exploration of its IT and electronic communications systems for business purposes, but discourages behaviour which may inconvenience other users.

1.3. IT systems include all computer systems and/or computing hardware and software (including associated peripherals) owned or explicitly approved for use by the CHC and any data stored therein.

1.4. Electronic communication includes, but is not limited to, any form of communications such as emails (including personal e-mails accessed through a web page), electronic forums and postings (e.g. blogs and wikis), web pages, instant messaging. It also includes access to the internet by staff and contractors through a Echogenicity device whilst away from the office, telephony communication and secure, remote access to the Cornwall NHS managed network (UAG/iChain, VPN, or such other form of remote access approved for use by the CHC).

1.5. Electronic forums include, but are not limited to, chat groups, discussion forums, news groups and social networking sites that allow the sending and receiving of text-based posts.

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

2. Purpose of this Policy/Procedure

2.1. The purpose of this policy is to define the permissible use of IT systems by authorised staff and contractors who have access to the Cornwall NHS managed network.

3. Scope

3.1. This policy applies to all users of IT systems in relation to:

- The use of IT equipment;
- The use of electronic communication;
- IT systems, leased, hired or otherwise provided by or to the CHC, connected directly or remotely to the Cornwall NHS managed network or used on Echogenicity's premises.

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 – Information is delivered to the right person, when it is needed.

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. 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 its criticality to Echogenicity) 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.

4.7. 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 Service Desk can be contacted by calling Extension 1717 (01209 881717) or non-urgent requests can be sent via email to CITS.ServiceDesk@cornwall.nhs.uk.

4.8. Cornwall Health Community (CHC) – all organisations with a connection to the Cornwall COIN (including Kernow Clinical Commissioning Group (KCCG), Royal Cornwall Hospitals Trust (RCHT), Cornwall Partnership NHS Foundation Trust (CFT), Peninsula Community Health (PCH), Echogenicity, GP's and other partner organisations).

4.9. Cornwall COIN – a CITS managed N3 community of interest network (COIN). This wide area network links all the computers across all Cornwall Health Community sites with the national N3 network.

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

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

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

4.13. 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.

4.14. 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 Community hardware and software.

4.15. HSCIC – Health and Social Care Information Centre.

4.16. IT – Information Technology is the application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data.

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

4.18. Mobile IT 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, e.g. laptops, tablets, Notebooks, PDA's, smart phones, etc.

4.19. N3 – The National NHS Network is a UK wide network connecting NHS organisations together (a private WAN)

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

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

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

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

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

4.22. 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

4.23. Recovery – Restoration of a system to its desired state following a failure in the operation of the system.

4.24. 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 Unified Access Gateway (UAG) which requires username, password and either a generated key from a Vasco token or a smartcard.

4.25. 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.

4.26. 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.

4.27. 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
- The Information Asset Owners of these systems have authorised access
- The associated system access documentation has been completed to enable the account to be processed by Cornwall IT Services
- Access to these systems are reviewed annually to ensure that it is still required.
- Ensuring that their staff are aware and compliant with this policy.

5.2. Role of the Information Governance Committee

The Information Governance Committee 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 Individual Staff

All staff members are responsible for:

- Ensuring that any usage conforms to policy and legislation relating to IT security, confidentiality and data protection.

- 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 manager and colleagues may need to gain access to an individual's IT systems under certain circumstances Staff and contractors are therefore advised to consider carefully the use of Echogenicity's provided IT systems for personal use.
- IT systems are a shared resource and each user has responsibility to learn how to use them appropriately
- Users are responsible for 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

6.1.1. Access to IT systems is primarily for business related purposes.

Personal use is permitted provided this does not interfere with the performance of your duties, those of other staff or contractors or the business of the Trust in general. Personal access to IT systems can be limited or denied by your manager. Staff and contractors must act in accordance with Trust Policy and their manager's locally imposed restrictions.

6.2. Unacceptable Use

6.2.1. If the monitoring tools show that a member of staff or contractor has been accessing material identified as indecent, obscene, offensive or otherwise inappropriate, the IT Security Manager will be informed who will raise the issue with the Trust Information Governance Lead. It is the responsibility of the IT Security Manager to ensure that the matter is dealt with in line with current IT Security Policy and procedures. This may result in a full enquiry that could result in disciplinary action being taken. If a breach is identified, the access of the staff or contractor involved may be suspended pending the enquiry conclusion at which point it may be terminated.

6.2.2. IT systems provided by the Trust should not be used:

- In contravention of the Data Protection Act and it's principles;
- In contravention of the Computer Misuse Act and it's principles;
- In ways that contravene the Human Rights Act
- for personal use, other than as permitted by the Trust;
- for the transmission of unsolicited commercial or advertising material, chain letters, press releases (unless specifically authorised by an Executive or the Head of Communications), or other junk-mail of any kind;
- for the unauthorised transmission to a third party of personal identifiable data or confidential material concerning the activities of Echogenicity;
- for the transmission of material such that this infringes copyright, including intellectual property rights;
- for the unauthorised provision of access to the Echogenicity's facilities by third parties;
- for activities that unreasonably waste time, network resources, disrupts the work of others or activities that unreasonably serve to deny service;
- for activities that corrupt or destroy data;
- for access, displaying, downloading, creation, storage or transmission (other than for properly supervised and lawful clinical or research purposes) of any indecent, obscene or offensive images, data, or other material, or any data capable of being resolved into obscene, offensive or indecent images or material;
- for access, displaying, downloading, creation, storage or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;
- for access, displaying, downloading, creation, storage or transmission of material that is abusive or threatening to others, or serves to harass, bully or personally attack others;
- for access, displaying, downloading, creation, storage or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, race, marital status, disability, political or religious

beliefs. Echogenicity is committed to fostering a working environment free of discrimination where everyone is treated with dignity, equality and respect;

- for access, displaying, downloading, creation, storage or transmission of: defamatory material; material that includes false claims of a deceptive nature; anonymous messages, i.e. without clear identification of the sender or material which brings the Trust into disrepute;
- for so-called 'flaming' i.e. the use of impolite terms or language, including indecent, obscene offensive or condescending terms;
- for activities that violate the privacy of others;
- for criticising individuals, including copy distribution to other individuals, unless undertaken as part of an approved and authorised HR process;
- for publishing to others the text of messages written on a one-tone basis, without the prior express consent of the author;
- to knowingly introduce viruses or other harmful programs or files (malicious software);
- to connect to any internal IT system without the permission of the appropriate owner;
- to attempt to gain deliberate unauthorised access to internal or external facilities or services (e.g. gaining access to another member of staff's email);
- to load software for which no legitimate licence is held.
- to promote personal views in a way which may be considered those of Echogenicity. (e.g. political lobbying)
- commenting or posting images on social media sites that could identify either a member of staff, a patient or a visitor.

6.2.3. Other than instances that demand criminal prosecution, Echogenicity is the final arbiter on what is or is not offensive material, or what is or is not acceptable use of IT systems.

6.3. User Names, Passwords and Smart Cards

6.3.1. 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.

6.3.2. Staff and contractors who have secure, remote access to the Cornwall NHS managed network have additional responsibilities and must abide by the Mobile IT Security Policy.

6.3.3. Staff and contractors should log out when finished with IT systems. Should a previous session be left unattended staff and contractors should log out from that session and commence their own. Any difficulties encountered whilst attempting this should be reported to the Cornwall IT Services (CITS) Service Desk.

6.3.4. All users issued with a smart card are responsible for complying with the terms and conditions as set out in the RA01 Form. Compliance will be monitored via line management arrangements, and Registration Authority Team audit. Any breach of these will be viewed as a disciplinary matter.

6.4. Unintentional Breaches of IT Security

6.4.1. 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.

6.5. Download of Files

6.5.1. All file downloads will be automatically virus checked.

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

6.6. The Use of the Organisation's Name

Office Mobile: 07590 234 865 Administrator: jemma.cassidy@nhs.net Visit: www.echogenicity.co.uk
Echogenicity Limited, 2 Beacon House, Beacon Road, St. Agnes, Cornwall TR5 0NE
Company Registration No: 5690772

6.6.1. If staff or contractors join an electronic forum they are expected to conduct themselves in an honest and professional manner. Individuals are responsible for what they write and should be courteous and inoffensive at all times. Staff and contractors are reminded to carefully consider whether to contribute to an electronic forum. Unless currently authorised to do so, staff and contractors are not permitted to write or present views on behalf of the Trust. For example; staff and contractors cannot join an electronic forum in the name of Echogenicity, nor can they design a web site and publish it under the name of Echogenicity.

6.6.2. Staff and contractors are also reminded to carefully consider whether to distribute or publish Echogenicity's e-mail address (such as when registering on third-party websites) as this may lead to the staff or contractors GroupWise mailbox being targeted by spam (commercial unsolicited e-mail) and phishing (fraudulent e-mails designed to aid identity theft) attacks or Echogenicity's systems being subject to attacks designed to prevent legitimate access and cause general disruption (Denial of Service).

6.6.3. Emails sent using the CHC email system include the organisations name and may be held to represent Echogenicity and its values. In exchanges of emails, staff could accidentally tarnish the image of the Trust and this policy aims to assist with the understanding of email good practice in an attempt to avoid this. Use of IT systems in such a way as to expose the Trust to risk of claims for defamation is prohibited.

6.7. Confidentiality

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

6.8. Contracts

6.8.1. Enforceable contracts may be formed over the Internet and e-mail, and staff and contractors are advised to take care to avoid entering into any commitments which they do not wish to be legally binding on them personally. Staff and contractors should ensure that they do not enter into contracts or give other commitments which would make Echogenicity responsible, unless they have authority to do so.

6.9. Periods of Absence

6.9.1. 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.

6.9.2. During unplanned periods of absence, such as ill health, or where access has not been given to a work colleague, a Director may formally request that CITS provide access to a staff member" s emails or documents, to minimise the disruption to service delivery. This must be authorised by Verity Williams-Curnow.

6.9.3. 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 on xt 1717.

6.10. NHS HSCIC Information Governance Toolkit

6.10.1. CITS, acting on behalf of the CHC, are responsible for helping to maintain a safe and secure IT environment. More specifically, they are responsible for providing evidence to demonstrate that Echogenicity conforms to the elements of the HSCIC Information Governance (IG) Toolkit that relates specifically to IT security.

6.10.2. The Director of CITS is responsible for providing the Chief Executive with an annual IG Assurance which will be confirmed by Verity Williams Curnow when submitting the IG Toolkit to Connecting for Health.

6.11. Monitoring Access

6.11.1. 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 and non clinical applications, internet and e-mail access, audio, video and other file downloads, blogs, wikis, postings and instant messaging. The IT Security Manager 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.

6.11.2. 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 Echogenicity's 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
- and to assure and protect the reputation of the Trust

6.11.3. Echogenicity 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.

6.11.4. Echogenicity 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.

6.11.5. 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.

6.12. Protection from Malicious Software

6.12.1. CITS will ensure, as far as reasonably practical, that every device owned or explicitly approved for use by Echogenicityhas 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.

6.12.2. 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 CHC.

6.12.3. 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 Echogenicity;
- 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

6.13. Reporting on Use

6.13.1. The IT Security Manager will provide regular IT security incident and monitoring update reports. These reports will be authorised by the Technical Services Manager and will be made available to Echogenicity.

6.13.2. If there appears to be excessive or inappropriate use of IT systems the IT Security Manager will be informed, who will raise the issue with Verity Williams-Curnow

6.14. Breaches of IT Security

6.14.1. 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.

6.14.2. Incidents and outcomes of any investigations will be reported to the appropriate organisational Information Governance Committee.

6.15. Information Security Incident Reporting

6.15.1. 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 1998.
- 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.

6.15.2. 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 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.

6.15.3. All incidents or information indicating a suspected or actual IM&T

security breach will be reported to the immediate line manager and the IT

Security Management Team via the CITS Service Desk.

6.15.4. 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.

6.15.5. 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.

6.15.6. The IT Security Management Team are responsible for immediately notifying any IM&T security incident to Verity Williams Curnow.

6.15.7. The IT Security Management 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 CHC" 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 Echogenicity's procedures.

6.15.8. The IT Security Management Team will record the incident on the Trust Incident Reporting System and on the CITS IT Security Risk Register.

6.15.9. The IT Security Management 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.

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

- provide Echogenicity's staff member with details of the planned investigation
- inform other key teams or staff members both within the CHC 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 Echogenicity 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 Echogenicity information governance 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.

6.15.11. The IT Security Management Team will complete the recording of the incident on the Trust Incident Reporting System and on the CITS IT

Security Risk Register by logging:

- date the IG Team was informed of the incident
- action taken by the IG Team
- follow up action needed to minimize or prevent the incident from re-occurring.

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

6.15.13. 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.

6.16. Action in the Event of a Breach of Policy

6.16.1. 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 Echogenicity policy and procedures and incident reporting procedures involving liaison between CITS and Verity Williams Curnow of Echogenicity.

6.16.2. 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.

6.16.3. 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.

6.17. Disclaimers

6.17.1. Echogenicity will supply an appropriate disclaimer that should be appended to all electronic communications that are sent external to Echogenicity.

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 CHC are compliant with the NHS Information Governance Toolkit (IGT).

Lead IT Security Management 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 Verity Williams-Curnow

Recommendations will be made by Verity Williams-Curnow.

Implementation action plans will be agreed by Verity Williams Curnow and 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.

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 IT Security Management Team will re -submit the Policy to

the organisations IGC/IGSC for consultation, ratification and dissemination.

9.3. Where the revisions are minor, e.g. amended job titles or changes in the organisational structure, approval can be sought from Verity Williams-Curnow responsible for signatory approval, and can be re-published accordingly without having gone through the full consultation and ratification process.

9.4. 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 Policy complies with Echogenicity's

Equality and Diversity statement which can be found in the 'Equality, Diversity & Human Rights Policy' or the Equality and Diversity website.

10.2. This Policy applies to all organisations within the Cornwall Health Community and will be reviewed by the organisations Information Governance Committee/Sub Committee to ensure compliance with the local Equality and Diversity Policies.

10.3. The organisation is committed to a Policy of Equal Opportunities in employment. The aim of this policy is to ensure that no job applicant or employee receives less favourable treatment because of their race, colour, nationality, ethnic or national origin, or on the grounds of their age, gender, gender reassignment, marital status, domestic circumstances, disability, HIV status, sexual orientation, religion, belief, political affiliation or trade union membership, social or employment status or is disadvantaged by conditions or requirements which are not justified by the job to be done. This policy concerns all aspects of employment for existing staff and potential employees.

10.4. Equality Impact Assessment

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

Links to key external standards

- Records Management: NHS Code of Practice
- Confidentiality: NHS Code of Practice
- The Data Protection Act 1998

- HMG Security Policy
- HSCIC IG 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
- The Mobile IT Security Policy
- Policy for the safe disposal of IM&T equipment and electronic media
- Malicious Software Policy
- 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