Information Security Policy

Version	**1.6**
Location	Policy Folder - Information Technology
Approving Committee:	Urgent Care 24 Board
Date Ratified:	March 2011
Reference Number:	UC24POL6
Name/Department of originator/individual:	James Carr, Director of Service Delivery
Name/Title of responsible committee/individual:	James Carr, Director of Service Delivery
Date issued:	17th March 2011
Review date:	January 2019
Target audience:	All Employees

Version	Date	Control Reason
1.2	20/11/2012	Reviewed in line with Information Governance submission. Changes made to job titles.
1.3	30/01/2013	Reviewed in line of annual revision and Information Governance submission.
1.4	10/12/2014	Reviewed in line of annual revision and Information Governance submission.
1.5	02/04/2018	Reviewed in line of annual revision and Information Governance submission.
1.6	31/08/2018	Update for changes in job title, building lease arrangements and GDPR

CONTENTS

1.0 INTRODUCTION

1.1 The need for an Information Security Policy

As a data controller Urgent Care 24 (UC24) holds and manages a great deal of personal and confidential data relating to patients, the public and UC24 employees. Increasing reliance is placed on Information Technology to store and manage this information and with ever-easier ways by which information can be passed around via UC24 and other connected networks it is important that a consistent approach is adopted to safeguard UC24 information in the same way that other more tangible assets are secured, with due regard taken to the highly sensitive nature of some information held on both electronic and manual systems.

This document describes UC24 policy on information security and employees' responsibilities for security of information held electronically and in hard copy format.

The Information Security Policy addresses the following issues;

- **Confidentiality:** Ensure that information is accessible only to those authorised to have access

- **Integrity:** Safeguard the accuracy and completeness of data and processing to ensure confidence in the authenticity of the information

- **Availability:** Ensure that authorised users have access to information and associated assets when required

This Information Security Policy is consistent with NHS Guidance, international standards and legislation and also supports Informatics Merseyside's Information Security Policy because UC24 uses the IT infrastructure which is owned by the CCG.

An information security Staff Checklist is in ***Appendix A.*** It is intended to help employees focus on the key areas that are likely to affect them on a day-to-day basis. The checklist should only be used once UC24 Information Security Policy itself is understood.

1.2 Purpose

This Policy is designed to be an overarching Information Security Policy for UC24. With its complete adoption it will ensure a safe and secure holding environment for electronic and paper based information.

1.3 Scope

This policy applies to:

- UC24 employees, at any location, at any time
- Associate Clinicians undertaking sessions on behalf of UC24 at any location, at any time
- Other persons working for UC24, persons engaged on UC24 business or persons using UC24 equipment and networks such as third party contractors
- All usage by anyone granted access to UC24 network

2.0 USEFUL DEFINITIONS

UC24: Urgent Care 24
IT or I.T: Information Technology
IM&T: Information Management & Technology IAO: Information Asset Owner
IAA: Information Asset Administrator SIRO: Senior Information Risk Owner
DPO Data Protection Officer
IA: Information Asset refers Applications, Equipment and Media used to access and hold information

3.0 GENERAL INFORMATION SECURITY POLICY STATEMENT

All of UC24 IT systems are secure and confidential. These are operated in accordance within NHS guidance, Caldicott Guidance and relevant legislation such as the Data Protection Act (2018)

All staff should make themselves are aware of this policy, the need to ensure appropriate secure and confidential handling of all personal and business sensitive information and their responsibilities in maintaining information security.

Confidentiality, integrity and availability of information should be maintained at all times. Employees will be trained in and adhere to the principles laid down in the Data Protection Act 2018, and other legislation and standards such as the Caldicott report and principles which govern information management procedures to detect and resolve security breaches are in place.
Failure by any employee of UC24, or any Associate Clinician undertaking work on the behalf of UC24, to adhere to the policy and its guidelines will be viewed as a serious matter and may result in disciplinary action

Where employees or Associate Clinicians believe that it is not possible to meet the policy and associated guidelines this must be brought to the

attention of the UC24 Director of Service Delivery who will manage the risk in accordance with the UC24 Risk Management procedure.

4.0 MANAGING INFORMATION SECURITY RISKS

Any information security measures must be viewed as a necessity to protect against a risk of an event occurring or to reduce the impact of such an event which will breach information governance. Some of these events may be deliberate acts of damage and others may be accidental. Nevertheless, a range of security measures can be deployed to address:

- The **Threat** of something damaging the confidentiality, integrity or availability of information held on systems or manual records
- The **Impact** that such a threat would have if it occurred
- The **Chance** of such a threat occurring

All staff should consider the risks associated with electronic and paper based Information Assets (IAs), and IT equipment and the information that is held on them.

All employees, Associate Clinicians and contractors are responsible for reporting any perceptible inadequacies of information security measures currently used by the Information Asset Owner.

5.0 ELECTRONIC AND MANUAL INFORMATION ASSETS/RECORDS

This section describes the policy and principles for storing and accessing computerised and paper based information and records owned by UC24.

5.1 Physical and Environmental Security

5.1.1 Premises

Access to equipment holding information located within UC24 managed property will be restricted through the use of the same precautions that are taken for other valuable assets of UC24. Such security measures and restrictions include perimeter security, CCTV, coded and lockable doors, secure windows, window blinds and screens, alarms, and signage.

Access to UC24 Headquarters is via coded external doors to the building and fob controlled, locked, doors to the UC24 premises.

Information systems that are particularly valuable or that hold or are used to access personal, sensitive and critical information should be located in rooms that have lockable doors. Where this is not possible,

e.g. mobile equipment, that equipment should be attended to by the users at all times where and when possible.

All IT equipment assets including hardware and software must be asset tagged and the serial number recorded on the UC24 asset register. The IT department will be responsible for maintaining this asset register.

Computer equipment belonging to UC24 and Informatics Merseyside must not be moved or disconnected without authorisation from the UC24 IT Department. No new and employee personal electronic/computer equipment may be connected to any network, including the internet, without the permission of the UC24 IT Department.

During the out of hour's period the Shift Managers will be responsible for enforcing this, the IT Department will support Shift Managers regarding this.

All employees, Associate Clinicians and contractors performing work on behalf of UC24 should take due care to make every effort to ensure that fire, flood, theft and accidents do not damage or result in the loss of IT equipment or manual information systems. Any suspected theft or damage to IT equipment should be reported to the UC24 IT Department.

All UC24 employees and Associate Clinicians must visibly wear the UC24 corporate identification badges and should challenge those colleagues and individuals not visibly wearing identification in controlled areas of UC24 premises. All contractors carrying out work on behalf of, and visitors to UC24, should be met at reception points where they are expected to "sign in" and be issued with a "Visitors" badge. Contractors and visitors should also be supervised at all times when moving round or working in controlled areas of the UC24 premises.

Heads of Departments will be responsible for notification of any new or returning employees to the UC24 IT Department to allow access rights to be appropriately established from effective dates. On the termination of employment, and in completion of work undertaken by contractors, ID badges must be returned and any keys returned used to gain access to controlled areas.

Heads of Department are responsible for notifying the HR Manager when members of staff leave the organisation so that the leaver's policy can be implemented, thus ensuring that there is no unauthorised access to UC24 information systems.

5.1.2 Storage

Paper based information assets are particularly vulnerable as they cannot be replaced as easily should they be lost, misplaced, or destroyed. When not in use all paper based information assets should be stored in secure filing systems away from electrical appliances and

other sources of heat to protect them against fire, flood, damage and theft.

Removable media such as CDs, DVDs, USB flash devices etc. should be encrypted using approved 256 Bit AES encryption software. When not in use these items should be stored in lockable cabinets and draws.

A clear desk policy should be adhered to by all staff and Associate Clinicians.

Excessive paper should not be stored on or near computer equipment and other sources of heat due to the risk of fire. IT equipment generates heat and needs adequate ventilation. Therefore all equipment must be sited to minimise the risk of accidental damage.

Other common hazards to IT equipment are drinks and food.

Disposal and Archiving of Information

Information that is no longer required should be disposed or archived securely and in line with the UC24 Records Management Policy. Paper records containing personal information must be disposed of securely.

Anything containing personal and/or confidential information that does not require archiving must be shredded after use. Any confidential information must be placed out of sight, preferably in locked cabinets when not in use.

The disposal of assets which hold or are used to access information, e.g. hard drives, fax machines, printers etc. must be stored securely whilst they are waiting to be destroyed.

The same principle applies to paper assets awaiting destruction.

Electronic data storage devices will be purged of all personal and sensitive information. Were it is not possible to purge electronic devices of personal and sensitive information they will be destroyed by an approved technical waste service provider. The UC24 IT Department will be responsible for the disposal of all IT equipment. The IM&T Standard Operating Procedure provides further guidance around disposal of asset equipment.

All paper records containing personal and sensitive information will be shredded using a “cross cutting” shredder or an approved shredding company. The disposal of paper based information is covered in a separate SOP which provides further guidance around shredding of paper based information assets.

UC24 will retain contractor’s receipts for all IT equipment and paper based records destroyed by compliant contractors on UC24 behalf.

For further guidance on the retention and disposal of health care records refer to the UC24 Records Management Policy.

5.2 Information Assets (IA)

Information Assets are identifiable and definable assets that are owned or contracted by an organisation which are regarded as 'valuable' to their business. As such these assets should have an assigned ownership to senior accountable staff known as Information Asset Owners (IAOs). Information assets (IAs) will likely include the computer systems and network hardware, software and supporting utilities.

Even the staff that are required to accomplish the processing of this data may be seen as both an important component part of the larger asset
e.g. Patient Administration System (PAS), or separately as an information asset in their own right. However, IAs should not be seen as simply technical or physical entities. There are many categories and components of IAs to consider including:

- Information – databases, system documents and procedures, archive media/data, paper records etc
- Software – application programs, system development tools and utilities
- Physical – infrastructure, equipment, furniture and accommodation used for data processing
- Services – computing and communications, heating, lighting, power, air-conditioning used for data processing
- People – their qualifications, skills and experience in the use of information systems and their availability
- Intangibles – for example, public confidence in the organisation's ability to ensure the confidentiality, integrity and availability of personal data

As these categories suggest, IAs are not necessarily tangible objects. Business processes and activities, applications and data should all be considered as IAs and/ or component parts. However, their degree of importance to the organisation may vary.

All UC24 employees, Associate Clinicians and contractors performing work on behalf of UC24 must comply with Data Protection legislation and must not be allowed to access information until the relevant departmental managers are satisfied that those individuals understand and agree these responsibilities. This will be included in all contracts of employment and service.

5.3 Ownership

Each designated critical and sensitive system will have a specified IAO (Information Asset Owner) who must ensure compliance with the

Information Security Policy, ensuring the appropriate use of equipment and the appropriate support and maintenance.

Each database or Information Asset (IA) will be recorded on the Information Asset Register. The IAO will have the ultimate responsibility for ensuring their IA is recorded and that they have a defined System Level Security Policy (SLSP). The SLSP documentation must include a clear statement as to the use of the IA, including users and detail about any restricted access to the IA.

5.4 Information Backup

Data located upon critical network servers will be backed up in accordance with the written back-up procedures to provide at least one month's information retention. Such information will be stored either off- site or in fire and flood proof safes as required. This will facilitate a maximum loss of one calendar week of information destroyed as a result of local building or system damage

All back-ups will be logged and maintained securely and will be erased when no longer required.

5.5 Business Continuity

All critical systems will have a written back-up procedure and disaster recovery plan. This is required to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

5.6 Access to Information Systems

Passwords and Codes

Passwords have a valuable role in protecting systems from unauthorised access and are most effective when they

- carry no meaning
- are not names or have other connections to the user
- are changed regularly and are not related to previous passwords
- are a minimum of 6 characters
- are a mixture of letters, numbers and symbols
- are kept secret
- are not 'VISITOR', 'GUEST' or similar
- are not shared

Passwords used within UC24 systems must be a minimum of 6 characters and must be changed at least every 90 days and deleted when a user no longer requires access to the system. A default password is used for accounts set-up by the UC24 IT Department. The user will then be prompted to change the password.

Only the person to whom it is issued should use that password. All UC24 employees must never divulge a password.

Only in exceptional circumstances (and not without the agreement of the Director of Service Delivery) will the IT Department change a password to grant temporary access. After which, a new password will be generated before further access to system.

A password policy will be developed with each SLSP to ensure security of access can be maintained and security of the original user account is not compromised.

5.6.2 NHS SMART Cards

NHS SMART Cards are issued to Urgent Care 24 employees who are authorised to access the NHS national programme the Personal Demographics Service. Employees must not under any circumstances share SMART cards or divulge their PIN number to anyone. The UC24 disciplinary policy will be used if SMART Cards are not used appropriately. Further guidance relating to SMART Cards can be found at the North Mersey HIS website http://nww.evoke.nhs.uk

6.0 INFORMATION TRANSMISSION AND NETWORKS

6.1 Local and Wide Area Networks

Through the connection of the UC24 network it is possible to receive and forward information to other users of the network and other external networks, for example through the use of electronic mail. Should employees receive, identify how to, or gain access to unauthorised information on any networks then this event must be reported to the IT Department.

A security log must be maintained of all access to UC24 network by external organisations. The IT Department will hold this log.

All computer files transferred from other networks (including public access networks such as the 'Internet') and removable media must be checked for viruses before use within UC24. Files stored on the network will be checked daily.

Any electronic equipment should not be used until advised by the UC24 IT department that the system is ready for use – such equipment includes mobile phones, USB flash drives, laptops, media players, CDs.

6.2 User Access to Network, Computers and Application

Only UC24 staff or authorised support agents such as Associate Clinicians and 3rd party support staff can legitimately access UC24 computers and the information held on them. Unauthorised access may contravene the Computer Misuse Act (1990) and Data Protection Act (2018) and other legislation leaving ***the user*** open to prosecution.

No individual will be given access to a live system unless properly trained and made aware of his or her security responsibilities.

Access to the network will be protected by passwords. Employees must be granted access only to those areas that they require to perform their duties.

A home working form must be authorised and sent to the IT Department to allow remote access for staff to be set up.

6.3 Web Services (Internet and Email)

Internet

UC24 regards the Internet as a tool for managing and delivering services, and as a useful mechanism for the open exchange of ideas and non-confidential sources of information between its employees, other members of the NHS and the public. The Internet can also be a wasteful resource in terms of the amount of time that it could consume if not used wisely or appropriately.
Staff using the Internet must ensure they comply with UC24 Internet and Email Policy

Heads of Departments and Managers will need to ensure that all staff read the Internet and Email policy.

Email

The office systems at UC24 are a valuable asset that enables employees to benefit from efficient office communication. Care should be taken when using electronic mail as the content can reflect poorly on the individual and UC24. E-mail is identical to any other form of UC24 business correspondence and can be legally binding or challenged.

All staff must adhere to the Internet and Email Policy

6.4 Notification of Staff Changes

Heads of Departments will be responsible for notification of new employees to the IT Department to allow access rights to be appropriately established from effective dates.

6.5 Security of Third Party Access to NHS Networks

Written agreement must be received from all external contractors and non-NHS parties that they agree to treat all information confidentially and within the law and that information will not be disclosed to unauthorised individuals. Such contractors should also sign the Confidentiality Agreement for 3rd Party Suppliers, showing that they understand the relevant legislation should they need to access sensitive information stored on a computer system.

6.6 Use and Installation of Software

Departments need to consult the UC24 IT Department in advance if any software, other than approved and authorised software is required to be loaded onto UC24 computers.

Employees must not bring or download software onto Urgent Care 24 premises without first getting permission from the IT Department.

It is a criminal offence to make/use unauthorised copies of commercial software and offenders are liable to prosecution.

All changes to and installation of software programs may only be undertaken by the IT Department.

'Games' software, except for the purpose of authorised training is not permitted for use on UC24 equipment and must not be installed or used on the premises.

6.7 Computer viruses

Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses.

Virus threats are a day-to-day threat however the type, strain and number of incidents may well increase due to the increased web activity.

This can cause serious disruption preventing access to critical systems and putting unnecessary strain both on the user and the IT Department

All UC24 personal computers must run anti-virus software

Employees or Associate Clinicians should not use computer media that has not been checked for viruses. Staff must contact the IT Department if a virus incident is suspected.

6.8 Clear Screen Policy

Workstations will require a username and password to be entered before accessing any software on that machine where the operating system permits. Further guidance can be found in the UC24 Clear screen policy.

6.9 Clear Desk Policy

Any confidential information must be placed out of sight in metal lockable cabinets when not in use to protect against fire, flood and theft.

7.0 PERSONAL USE OF URGENT CARE 24 SYSTEMS

All computer equipment leaving UC24 premises should be authorised by the UC24 IT Department and a copy of the signed equipment off site form must be filed by the IT Department.

8.0 MANAGEMENT OF MANUAL RECORDS

8.1 Relevant Filing System

The Data Protection Act covers not only personal data attributable to a Living person held in an automatically process-able form but also personal information which is recorded as part of a 'relevant filing system'.

Information recorded as part of a 'relevant filing system' is a structured set of information that can reference individuals either directly or indirectly so that 'specific information relating to a particular individual is readily accessible'. This definition covers some types of paper-held data.

Further information is available in the Urgent Care 24 Records Management Strategy and Records Management Policy.

More detailed information relating to the Data Protection Act (2018) can be found in the UC24 Confidentiality, Data Protection and Caldicott Policy.

8.2 Sharing of Personal and Sensitive Information

Information relating to individuals should not be shared without following the Information Governance guidance for sharing information safely and legally. Further guidance is provided on how information should be transferred is provided in the UC24 Confidentiality, Data Protection and Caldicott Policy.

9.0 SPECIFIC DUTIES & RESPONSIBILITIES

9.1 Introduction

This section describes the different areas of responsibilities for ensuring that UC24 data and IT assets remain secure. There is a clear division of responsibilities between the Board, Executive Directors, IT Department, Line Managers, and employees.

9.2 Urgent Care 24 Board

UC24's Board has overall responsibility for all matters relating to information security. Board membership includes Executive and Non- Executives. All matters concerning security should be referred to UC24's Director of Service Delivery or the Data Protection Officer.

9.3 Executive Directors

Executive Directors and Heads of Departments should:

- Ensure there is sufficient resource available for securing information assets and training staff
- Ensure that all current, new and temporary staff are instructed in their security responsibilities and receive appropriate training
- Ensure that contractors undertaking work on behalf of UC24 are aware of and comply with UC24's standard operating procedures for information security
- Ensure that all their staff using computer systems/media are trained in their use
- Ensure that no unauthorised staff are allowed to access any of UC24's computer systems or information stores because unauthorised access could compromise information integrity
- Determine which individuals are to be given authority to access specific information, levels of access to specific systems should be on a job function need, independent of status
- Ensure that the IT Department are notified of new employees to allow access rights to be appropriately established from effective dates
- Authorise new information systems ensuring they provide an adequate level of security and do not compromise the existing infrastructure or pose a risk to the organisation
- Implement procedures to minimise UC24's exposure to fraud, theft, or disruption of its systems, such as segregation of duties, dual control or staff rotation in critical susceptible areas
- Ensure that current documentation is always maintained for all critical business processes to ensure continuity in the event of individuals being unavailable.
- Ensure that staff are aware of UC24's position on potential personal conflicts of interest
- Ensure that all staff employed by UC24 sign confidentiality (non- disclosure) undertakings as part of their contract of employment and ensure that all staff sign and return ***Appendix A*** of this document

- Ensure that all 3rd parties and contractors undertaking work on behalf of UC24 complete and sign The Confidentiality Agreement For 3rd Party Suppliers

9.4 IT Department

The IT Department for UC24 in conjunction with senior management staff is responsible for the implementation and enforcement of the Information Security Policy and has organisational security management responsibilities for:

- monitoring and reporting on the state of Information Management & Technology (IM&T) security within UC24
- ensuring that the Information Security Policy is implemented throughout UC24's Information technology systems
- developing system level security policies
- enforcing detailed procedures to maintain the security of IT systems
- ensuring compliance with relevant legislation and standards relating to the governance of information management and security
- monitoring for actual or potential information security breaches
- conforming to the Information Security Policy
- reporting IT related security issues to the Director of Service Delivery
- providing an advisory service on information security for IT systems
- understanding the risk to the computer assets and the information that is held on them
- deploying appropriate security measures to reduce identified risks with the aim of reducing the impact of those risks should they materialise
- ensure that a contingency is in place to manage security issues
- periodically review security for IT systems
- ensuring that new information systems provide an adequate level of security and do not compromise the existing infrastructure
- ensuring that procedures are in place so that heads of departments or human resources department advise the IT department immediately about staff changes affecting computer access (for example job function changes/leaving department or UC24) so that passwords may be withdrawn / deleted
- ensure that the IT Department maintain security in line with the information security policy
- ensure that incident reporting protocols are followed

Note: systems are liable to independent reviews by internal and external auditors.

9.5 Senior Information Risk Owner (Director of Service Delivery)

Is the SIRO for managing information risk at the executive level and is therefore responsible for managing any identified risk relating information security.

9.6 Data Protection Officer (Company Secretary)

In accordance with the Data Protection Act 2018 UC24 has a Data Protection

Officer who holds overall responsibility for compliance and reporting in relation to information governance.

9.7 Information Asset Owner

Has delegation responsibility for managing any information on any information assets they own.

9.8 Information Asset Administrator

Whilst the IT Department will maintain user account access control for all IT Systems, the IAA's will be responsible for compliance with this Information Security Policy to maintain controls in order to provide:

- optimum confidentiality of information
- optimum system integrity
- optimum availability of information
- appropriate use of equipment by appropriately trained personnel
- system security reviews

9.8 Heads of Department and Shift Managers

Heads of Department and Shift Managers are:

- required to conform to the Information Security Policy
- ensure that UC24's personnel are aware of their responsibilities and accountability for information security
- required to ensure their staff are working in a manner consistent with the Information Security Policy
- responsible for investigating any security issue that members of staff raise in connection with their work
- responsible for addressing unresolved information security issues with the IAO
- required to ensure that staff have signed their contract indicating that they understand and will comply with the Data Protection Act (2018) and Caldicott guidance and will also comply with other legislation highlighted in the UC24 Confidentiality, Data Protection and Caldicott Policy
- ensure compliance with the Computer Misuse Act (1990) and the Copyright Designs and Patents Act (1988)

9.9 Staff

All staff are responsible for ensuring that no actual or potential information security breaches occur as a result of their actions.

Employees and Associate Clinicians, including those under contract and agency staff, are:

- responsible for conforming to the Information Security Policy
- required to bring to their manager or IT Department's attention any areas of concern regarding information security
- required to abide by the terms of the Data Protection Act (2018) and Caldicott guidance, and also comply with other legislation highlighted in the UC24 Confidentiality, Data Protection and Caldicott Policy
- ensure compliance with the Computer Misuse Act (1990), and the Copyright Designs and Patents Act (1988)
- Have an understanding of the importance of data quality and partake in training offered on systems

9.11 Information Security Incident Management

The DPO (Data Protection Officer) will oversee investigations into all suspected and actual information security breaches in liaison with the SIRO (Senior Information Risk Owner). All investigations will be conducted in line with the UC24 Incident Reporting Procedures.

Security breaches may result in disciplinary action.

10.0 CONTACT INFORMATION

10.1 Information Security

The IT Department has a responsibility for information security.

The IT Department provide support and guidance for UC24 on all issues concerning information security. Advice regarding information governance matters such as Data Protection and Caldicott can also be taken from the Clinical Governance Manager in conjunction with the IT Department.

I.T Department 09:00 to 17:00 Monday to Friday Telephone: 0151 254

2553

11.0 TRAINING REQUIREMENTS

As this policy is an overarching policy, the training on its content is delivered via a number of different areas. This includes the induction training for new starters, UC24 information governance training, and Caldicott awareness training and other internally arranged courses.

12.0 REVIEW AND MAINTENANCE

This policy will be subject to annual revision and, if revised, all staff will be alerted to the new version.

This policy is maintained by the UC24 IT Department on behalf of UC24

Please consult your Manager or the IT Department if you have any queries.

The latest version can be found on Urgent Care 24 Intranet

Appendix A

Information Security Agreement checklist and sign off

This agreement is intended to be a helpful Information Security aide-memoir for employees. It is not intended to be a comprehensive summary of user responsibilities and does not reduce or alter the standards or principles in the Information Security Policy.

Employees should:

- Contact the IT Department if you are aware that you are not meeting the standards and principles of the Security Policy
- Be aware of the potential risks that surround the data and systems you use. Do consider the security measures that you currently use in relation to these risks
- Store all sensitive information on central file servers and not on personal computers if facility available
- Safeguard portable IT equipment. Do not leave them visible and unprotected in public places. Portable hardware must be installed with password protection. Please contact the IT Department.
- Dispose of any confidential data, on printouts or computer media, securely
- Log off and use a password protected screen-saver, if you leave a computer
- Use email professionally. As if writing on the organisations own letterhead
- Be aware of other organisation's related policies, including the internet and email policy
- Wear your staff identification badge at all times
- Ensure they have read and understood the guidance for sharing personal information contained in **Appendix A.** Any queries should be directed to your Manager or the IT Department**.**

Employees should not:

- Move ANY non-portable IT equipment without contacting the IT Department.
- Use e-mail for clinical or confidential information without consulting the IT Department
- Share passwords or use someone else's password
- Hold personal data on your own system without understanding the Data Protection Act and Principles and confirming that there is sufficient physical security in place (e.g. lockable doors)
- Copy personal data from one system to another without confirming that the recipient system has the same or greater security protection
- *Use or try to use IT networks which you have not been authorised to use

- Use ANY non authorised external memory stick, USB pen, MP3 Player or similar device on ANY UC24 network computer system
- *Install or make copies of ANY software. IT should be consulted. Copying software must be done with the authority of the copyright holder.
- Store confidential information on portable IT equipment such as Laptops and Pen drives without encryption being used

Relevant Legislation

Computer Misuse Act 1990

Copyright Designs and Patents Act

I confirm that I have read, understood and accept the above.

Signature…….

Print Name……...

Date……...

Appendix B

Access and Support to the Computer Network and From External Third Parties

1. INTRODUCTION

This document outlines the Policy and steps to be taken in reference to access to the organisations network and computer systems by external third parties typically providing IT support.

The Security Policy is the master document and reference. This guidance is designed to clarify the key issues assisting staff and contractors to maintain and keep to UC24 Security Policy and associated NHS Wide Network (NHSnet) Code of Connection.

2. Policy Statement

All access by third parties to be managed under a clear protocol agreed with the IT Department and supervised throughout.

All connections wherever possible should be made through the NHSnet

Onsite support is to be provided by nominated, identifiable individuals in the supplier's firm. All on site staff to conform to local site security by wearing ID badges and only be permitted to areas required.

All work by external companies to be closely monitored with activities logged.

All support contracts must include a specific statement on the supplier's responsibilities with regard to their employees' actions and protection of the support mechanisms (including the software, hardware and access configuration details). This should state any penalties for breach of confidentiality or integrity by the supporting organisation.

3. Procedures

Each service call must be authenticated. The highest level of authentication mechanisms available should be used.

Access is to be controlled through the use of a unique user identifier and password.

The access point (modem or network connection) is disabled unless support is required. For example the modem should be switched off and via NHSnet the Firewall rule permitting access must be set to 'drop/no access'.

Checks on any changes made are to be carried out before the system is made operational again, including detection of computer viruses.

4. Data and Network Service Protection

- Host system controls must be in place to prevent unauthorised access to sensitive data or;
- All sensitive data and applications are removed from the system during support or;
- All confidential data or sensitive applications are protected by data encryption.

Access to connections both for the local and wide area network is prevented to service personnel or; the links are disabled during the support period.

5. References

NHSnet Code of Connection
NHS Information Authority Code of Connection
NHS Information Authority Security and Access Policy
NHS IM&T Security Manual

Appendix C

Accessing N3

The organisation is connected to the NHS Wide Network providing managed access to:

World Wide Web (Internet) services

In addition it supports connection between organisations and other networks.

The organisations connections to N3 are regulated through the NHS Code of Connection. The Code of Connection confirms that a NHS organisation has effective security measures in place and is audited and monitored by the Telecoms Branch of the Information Health Authority.

Good practice, along with other advice and guidance developed by the Information Health Authority can be accessed via the NHS Web Site.