

---

# IT Shared Services for PT & PCT's Within Gloucestershire

---

## Section A2: IT Security Policy

Approved By:	B. Wood Head of IT Shared Services	Signature:  Date:
	Information Governance Group	Signature:  Date:
	GPT Board Representative	Signature:  Date:



## Contents

- 1. Introduction ..... 5
  - 1.1 Need
  - 1.2 The aims
  - 1.3 Scope
- 2. Security Organisation & Responsibilities ..... 7
  - 2.1 Introduction
  - 2.2 Security Roles
    - 2.2.1 Department Managers
    - 2.2.2 Application System Managers
    - 2.2.3 Data Owners
    - 2.2.4 IT Shared Services
    - 2.2.5 Staff
  - 2.3 Security Incident Management
    - 2.3.1 Reporting of Software errors
    - 2.3.2 Reporting of Security weaknesses
- 3. Computer Information Systems .....12
  - 3.1 Physical Security
    - 3.1.1 Building Security
      - 3.1.1.1 Entry Controls
    - 3.1.2 Equipment Security
      - 3.1.2.1 Equipment sitting & Protection
      - 3.1.2.2 Equipment Maintenance
      - 3.1.2.3 Power Supplies
  - 3.2 Disposal of Equipment & Media
    - 3.2.1 Equipment
    - 3.2.2 Media
  - 3.3 Data Storage
  - 3.4 Data Backup
    - 3.4.1 Centrally Hosted Servers, Applications
    - 3.4.2 Local Department or Site Servers
    - 3.4.3 Management of Media
  - 3.5 Disaster Recovery

- 3.6 System Ownership
- 3.7 Software Licensing
- 4. Data Transmission & Networks .....16
  - 4.1 Local & Wide Area Network
  - 4.2 User Access
  - 4.3 Internet & Email Access
    - 4.3.1 Internet Access
    - 4.3.2 Email Access
    - 4.3.3 Rights, Obligations & Responsibilities
  - 4.4 Staff Changes
  - 4.5 Third Party Access
    - 4.5.1 Contractors
    - 4.5.2 Third Party
- 5. Desktop ..... 20
  - 5.1 Use & Installation of Software - Licensing
  - 5.2 Computer Virus Controls
    - 5.2.1 Definition of a Computer Virus
    - 5.2.2 Risks
  - 5.3 Password Rules
  - 5.4 Clear Screen Policy
  - 5.5 Personal Use of NHS organisations Systems
- 6. Tele-working/home working .....23
  - 6.1 Introduction
  - 6.2 Definition of Teleworking
  - 6.3 Definition of Homeworking
  - 6.4 Definition of Mobile Devices
  - 6.5 Record of Home, Mobile Users
  - 6.6 Use of Person Identifiable Data
  - 6.7 Connection to NHSnet remotely
  - 6.8 Use of Privately owned mobile devices and computers
  - 6.9 Legal Liability
  - 6.10 Home Workers – Health & Safety
- 7. IT Department ..... 28
  - 7.1 Useful Contacts
- Appendix A Security Incidence Form ..... 29
- Appendix B Network Use Agreement Form ..... 32
- Appendix C Confidentiality Agreement – Contractors ..... 34
- Appendix D Confidentiality Agreement – Third Party ..... 35

Appendix E Mobile, Home Computing & Tele-Working ..... 36

## 1. INTRODUCTION

This document describes the PT & PCT IT Shared Services within Gloucestershire, policy on information security and employees' responsibilities for security of information held or processed electronically on computers.

### 1.1 The Need

The IT Security Policy exists to safeguard electronically processed data, to meet legal requirements and to satisfy obligations to the NHSIA, clients and staff. It recognises security threats to information systems and provides a framework for reducing the likelihood of security incidents.

This document addresses the following issues:

- |  |  |
|--|--|
| <ul style="list-style-type: none"> <li>▪ Confidentiality</li> <li>▪ Integrity</li> <li>▪ Availability</li> </ul> | <p>Ensure that information is accessible only to those authorised to have access</p> <p>Safeguard the accuracy and completeness of information and processing to ensure confidence in the authenticity of the information.</p> <p>Ensure that authorised users have access to information and associated assets when required.</p> |
|--|--|

The IT Security Policy is consistent with and supports the NHS organisations policies and existing methods of working, including Standing Orders and Standing Financial Instructions which take precedence on any specific issue, and is in accordance with NHSIA national guidance.

### 1.2 The Aims

- All of the NHS Organisations computer systems are secure and confidential. In particular that these are operated in accordance within NHSIA policy guidelines, BS7799, Caldicott Guidance and relevant legislation such as the Data Protection Act (1998). To understand this issue more, refer to the NHS Organisations Information Security Policy.
- All staff 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 are maintained.
- Employees adhere to the principles laid down in the Data Protection Act (1998) and the Caldicott Report.
- Procedures to detect and resolve security breaches are in place.

Where employees believe that it is not possible to meet the policy and associated guidelines this must be brought to the attention of the IT Network Security Manager and action agreed and notified to the appropriate management level within the NHS organisation.

Failure by any employee of the NHS organisations to adhere to the policy and its guidelines will be viewed as a serious matter and may result in disciplinary action under

the NHS organisations Human Resources policies. Please refer to the current HR policies for up-to-date information.

### **1.3 Scope**

The scope of this policy covers the following areas:

- Safeguarding the NHS organisations electronic records from loss, destruction or falsification.
- Compliance with data protection and other legislation.
- Security Incident reporting and Investigation support.
- Control of the copying of proprietary software.
- Virus and Anti-Malware detection and prevention
- Control of access to the NHSnet
- Compliance with the NHS organisations Information Security Policy.

**For advice on any part of this policy, please do not hesitate to seek advice from the IT Shared Services Network Security Manager, who can be contacted via the IT Helpdesk.**

## 2. SECURITY ORGANISATION AND RESPONSIBILITIES

### 2.1 Introduction

Security is everybody's business and therefore it is everybody's responsibility to ensure information is, as appropriate, confidential, accurate and available to authorised users. This section describes the different areas of responsibility and roles within the IT Shared Services that affect IT Security Policy.

The NHS organisations Information Security Manager (or Officer, or IM&T Lead), needs to approve this IT Security Policy as part of compliance with Information Governance (which includes BS7799), as advised by the NHSIA.

The IT Network Security Manager is responsible for developing, implementing and monitoring the IT Security Policy for the IT Shared Service.

This document will be reviewed annually by the Head of IT Shared Services (PT & PCT's), with input from the IT Network Security Manager and other specialities within the IT Shared Service. There will also be an ongoing review of the IT Shared Services policies and operational procedures against this policy and feedback reported to the Head of IT Shared Services (PT & PCT's).

### 2.2 Security Roles

The responsibility of the various aspects of Information Security is shared between staff in the IT Shared Services team in order to cover the wide physical dispersion of the PT & PCTs sites, including GP's surgeries. Copies of the relevant Information Security documents are to be made available to each NHS organisation and nominated security personnel.

#### 2.2.1 Department Managers

Department Managers as the budget holders are responsible for all computer equipment and peripherals in their department, i.e. visual display units (VDUs), printers, scanners, personal computers (PCs) etc. In detail their responsibilities include:

##### Equipment:

- Maintenance of a register of all computers in their department/site.
- Physical safety of all computers and peripherals.
- Ensuring correct installation of consumables, e.g. printer ribbons, toner cartridges, etc.
- Ensure that the purchasing of new equipment is made in line with NHS organisation procurement requirements.
- Ensure appropriate virus checking software is in place.
- Logging and reporting of security incidents.

**Staff:**

- Ensuring all staff use systems and equipment securely and have training made available for them to do so.
- To enable all staff within their department/site comply with the NHS organisations Information Security policy and procedures.
- Upon staff termination of employment, departmental property is returned including identity badges and any user rights are removed from IT Shared Services systems.

**2.2.2 Application System Managers**

Each software application (i.e. PAS, SMARTSTREAM, SUNRISE CLINICAL MANAGER, CHILD HEALTH, etc.) is controlled by a named Application System Manager whose name should be registered with the IT Shared Services.

Where Application System managers are IT Shared Services staff, they are responsible for the running of the system and for the integrity of the data, i.e. data ownership.

Where Application System Managers are non IT Shared Services staff, a Data Owner should be identified and registered.

Responsibilities of Application System Managers:

- Control of access to the system, i.e. setting up user accounts and allocating access levels and passwords.
- Removing accounts when staff terminate their employment.
- Ensuring the delivery of appropriate user training in both the use of the application and the security aspects of the application.
- Agreeing fixes and upgrades to the system.
- Liaison as appropriate with the IT Shared Services.
- Ensuring system procedures are documented.
- Evaluating operational procedures to identify potential security risk(s).
- Recording and acting upon security violations of the system.
- Ensuring that output from the system is distributed securely.

**(Functions with high security risk should be performed by 2 persons to avoid fraud or misappropriation.)**

**2.2.3 Data Owners**

Where Application System Managers are not IT Shared Services staff, a Data owner needs to be identified. Their responsibilities include:

- 'Ownership' of the data, i.e. responsibility for data integrity.

- Liaising with the IT Shared Services regarding system access problems.
- Liaising with the Application System Manager regarding operational procedures.
- Supporting other users of the system.

### **2.2.4 IT Shared Services**

- The IT Shared Services is responsible for planning and maintaining the local area network and associated wide area network links.
- The IT Shared Services IT Network Security Manager is responsible for ensuring compliance with the IT Security Policy. This will be achieved by conducting regular random site spot checks.

### **2.2.5 Staff**

Each member of staff (including those under contract, agency, casual and bank staff), is:

- Accountable for the function they perform and each has a responsibility to ensure compliance with the NHS organisations Information Security Policy and procedures.
- Required to bring to their manager or the nominated Security Officers attention areas of concern regarding information security.
- Required to abide by the terms of the data Protection Act (1998) and Caldicott guidance, plus compliance with other legislation.
- Ensure they have familiarity with anti-virus measures and such software is being maintained with regular automated updates.

## **2.3 Security Incident Management**

In principle, a security incident is any breach or potential breach of information/security, physical or computer related. Damage to the NHS organisations from security incidents can be minimised by monitoring and acting upon such incidents. All NHS staff, contractors/agency, must report any observed or suspected incidents as detailed below.

### **2.3.1 Reporting of Software Errors**

#### **Application Software**

Users of application software should report any functional error to the system manager for the application.

#### **PC Software**

Users of PC's should report any suspected Virus or other Mal-ware to the IT Helpdesk.

Users of PC applications, which are supported by the IT Shared Services, should report any problem with applications to the IT Helpdesk for PC support staff to resolve.

Users of PC applications, which are **NOT** supported by the IT Shared Services, may seek advice from the IT Helpdesk, but should ensure that a suitable source of assistance is available from the supplier of the application.

### **2.3.2 Reporting of security weaknesses**

Users of the IT Shared Services network should report any observed or suspected security weaknesses to their line manager who will then assess the significance of the incident. The Incident Report Form should be completed. (see **Appendix A**). Once the line manager has assessed the incident he/she will take appropriate action according to the seriousness of the incident.

#### **Examples of the type of incidents to be dealt with by Line Manager:**

- Disclosure of password to another person within the PCT with same system access levels.
- PCs/VDUs left logged in and unattended in secure areas, i.e. not open to the public.
- Printer output not distributed, i.e. left on the printer in secure areas, not open to the public.
- The integrity of the system or data being accidentally put at risk.

#### **Examples of more serious incidents that must be reported to the Information Security Manager (or nominated Security Officer):**

- Disclosure of confidential information to any unauthorised individual.
- Disclosure of password to another person in or outside the NHS organisation, which could enable unauthorised access to computer systems.
- Attempted unauthorised access to computer systems.
- PCs/VDUs left logged in and unattended in public areas.
- Printer output not distributed, i.e. left in an insecure area and accessible to unauthorised individuals.
- The integrity of the system or data being deliberately put at risk.

## 3. COMPUTER INFORMATION SYSTEMS

### 3.1 Physical Security

Resources associated with information processing, such as offices, buildings, computer equipment, electronic services, communications media and paper-based records shall be protected from unauthorised access, misuse, damage or theft.

#### 3.1.1 Building Security

All IT Shared Services facilities that support critical and sensitive business activities should be housed in secure areas. These facilities should be physically protected from unauthorised access, damage and interference.

Rooms should be lockable and windows secure to break-ins.

In vulnerable areas, the installation of an alarm system should be considered as well as mechanism to physically secure equipment so that it is difficult to remove.

##### 3.1.1.1 Entry controls

- Digital lock numbers on doors should only be available to authorised staff.
- All staff to have physical identification.
- Visitors should be supervised and required to wear a visible authorisation badge and their date and time of entry and departure recorded.

#### 3.1.2 Equipment Security

##### 3.1.2.1 Equipment sitting and protection

- PCs must be kept in secure environments and kept out of sight of from the public as far as possible.
- Screens must be positioned so that no unauthorised viewing of confidential information can take place.
- Users must lock their workstation when left unattended for any length of time.
- Password protected screen savers should be used whenever it is likely a workstation will be left unattended. Screen savers must be set to operate at seven minutes within sensitive locations and an absolute maximum of 15 minutes inactivity at other locations.
- Applications must be closed/logged out before the user leaves the workstation.
- Printer output must be handled securely, i.e. immediately filed or distributed and therefore not visible to anyone who is not authorised to see the data.
- Any eating or drinking must take place in a way that minimises the risk of damage to equipment (e.g. keyboards).

### 3.1.2.2 Equipment maintenance

- According to assessed risk, maintenance agreements for all equipment should be taken out.
- If appropriate, maintenance agreements must include a confidentiality clause to ensure data security.
- Only authorised staff should be allowed to work on hardware or software, i.e. IT Shared Services staff or authorised contractors. Contractors should be escorted and supervised whilst on site.

### 3.1.2.3 Power Supplies

- Critical equipment should be protected from power outages/brownouts or other electrical anomalies.
- Power and telecommunications lines into IT facilities should be protected against electrical anomalies.

## 3.2 Disposal of Equipment & Media

### 3.2.1 Equipment

When considering the disposal of computer equipment, attention must be drawn to the Information Security issues surrounding the equipments use.

The hard disk on a PC or server is used to store information. Should personal data as defined under the Data Protection Act (1998), or any sensitive NHS organisation data such as accounting or HR, has ever been processed on that machine then precautions must be carried out to ensure that the information is not accessible to unauthorised persons after the machine is decommissioned.

Before disposal of a PC/laptop, the hard disks contents must be cleared. This has to be arranged through the IT Helpdesk who will arrange for the work to be performed to the standards laid down by the NHSIA policy. A Destruction Certificate will be issued stating that all data on the disks has been destroyed to an unrecoverable state.

In the case of transfer of ownership of a PC/laptop it is wise to have the hard disk contents cleaned of previous data. This can be arranged through the IT Helpdesk who will arrange for a software routine to be used on the machine. See IT Shared Services operational procedure **C15: Disposal of Equipment & Data Destruction**.

### 3.2.2 Media

The following list identifies typical computer media that requires secure disposal:

- CD/DVD and floppy disks.
- Magnetic tapes/cartridges used for backups.
- Voice & video tapes/cartridges used in surveillance systems.

The relevant NHS organisation policy (Records Management Strategy) held by the Information Security Manager should be consulted for the correct means of disposal.

### **3.3 Data Storage**

Sensitive information must **NOT** be stored on individual drives on PCs. This information is to be stored on the network servers where available, with access strictly controlled by access permissions.

Should a need arise for local temporary storage, then the IT Helpdesk must be contacted to approve and instruct on adequate physical security and backup arrangements.

If information is copied between systems on the network, then users should ensure that any confidential information remains secure and that the recipient system has the same or greater standard of security protection as the first.

### **3.4 Data Backup**

#### **3.4.1 Centrally Hosted Servers, Applications**

Data located on central network servers will be backed up in accordance with written procedures. Such data will be stored securely, off-site as necessary, according to a risk analysis for disaster recovery purposes.

Backups should be arranged to provide at least one month information retention for critical systems.

All backup media will be maintained securely and erased securely when no longer required.

#### **3.4.2 Local Department or site servers**

Data located on departmental or site specific backup servers will be backed up in accordance with written procedures. The responsibility for these data backup systems lies with the Departmental manager or site security person. IT Shared Services will supply technical and support services if requested.

Backups should be stored securely, off-site as necessary, according to a risk analysis for disaster recovery purposes, to facilitate a maximum loss of one calendar week of information destroyed as a result of local building or system damage.

Backups should be arranged to provide at least one month information retention for critical systems.

All backup media to be maintained securely and erased securely when no longer required.

#### **3.4.3 Management of Media**

All media containing data, i.e. disks, tapes, CD/DVD-ROMS, etc., containing important data (system, application software, data files, archives) must be stored in a safe secure environment and erased securely when no longer required.

This to cover media (CD or DVD) copies of all licensed software which must be inventoried to assist in audits and Disaster Recovery procedures.

### 3.5 Disaster Recovery

All designated sensitive and critical systems should have a written back-up and disaster recovery plan. This is required to protect the IT Shared Services operational and informational needs. These systems will be reviewed periodically by the IT Shared Services and the NHS organisations Information Security Officer to cover the organisations risk analysis and business needs. See the following IT Shared Services documents for more details;

**A6: IT Disaster Recovery Plan**

**C9: IT Disaster Recovery Procedure**

### 3.6 System Ownership

Each application sourced on or across the IT Shared Services network will have a specified system manager who must ensure compliance with the Information Security Policy, ensuring the appropriate use of equipment, support and maintenance.

Where a system manager is a member of the IT Shared Services they still need to maintain controls to provide:

- Optimum confidentiality of information
- Optimum system integrity
- Optimum availability of information
- Appropriate use of equipment by appropriately trained personnel
- System security reviews.

### 3.7 Software Licensing

An up-to-date software inventory is to be maintained by the IT Shared Services department for auditing purposes whether internal or external. This inventory to record the number of licensed software copies in use and where installed, along with licence details such as licence number, date valid and version number. Failure to maintain an up-to-date software inventory increases the risk of litigation, due to the inability to provide sufficient evidence of licensing arrangements.

A regular audit for unauthorised and unlicensed software to be performed to confirm that only correctly licensed software is in use on computers under the control of the IT Shared Services department.

## 4. DATA TRANSMISSION & NETWORKS

### 4.1 Local & Wide Area Networks

Access to the IT Shared Services network (LAN & WAN) for associated NHS organisations within the County of Gloucestershire will be protected by passwords.

Users will be granted access only to those areas that they require to perform their duties. Details of and control of access is contained in the IT Shared Services operational procedures document **C7: Access Control**.

Normal user access is given to the Internet and E-mail. More security information is given in the policy document **AUP3: Internet & E-mail Acceptable Use Policy**.

Through connection to the IT Shared Services network it is possible to receive and forward information to other users of the network and other organisations' networks using, for example, electronic mail. Should users receive, identify how to, or gain access to unauthorised information on any networks then this event must be reported to the Information Security Manager.

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

A security log must be maintained of all access to the IT Shared Services network by external organisations. The IT Helpdesk will hold this log.

Access for configuration to the infrastructure network devices, (Routers, Modems, Firewalls, etc.) shall be protected by passwords. Modem links must use strong authentication like CLI, and CHAP.

Connection to the NHSnet shall follow the NHSIA Code of Connection (2002) and the related controlling policies issued by the NHSIA. These can be referenced at <http://nwww.nhsia.nhs.uk/security/pages/default.asp>

### 4.2 User Access

Only NHS organisations staff, casual and bank, or authorised support agents are authorised to access the NHS organisations computer systems and the information held on them. Unauthorised access will contravene the Computer Misuse Act (1990) and Data Protection Act (1998) and other legislation leaving **the user** open to prosecution.

Before access is given to a User account, users must complete a Network Use Agreement form. This is given in **Appendix B**.

## 4.3 Internet & Email Access

### 4.3.1 Internet Access

The local NHS organisations regard the Internet as a tool for managing and delivering services, as a useful mechanism for the open exchange of ideas and non-confidential sources of information between its staff, other members of the NHS and 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 must not download software from the Internet for use on Trust owned computers without authorisation from the IT Shared Services Helpdesk. This includes shareware and trial or demo software. Only licensed software to be used on Trust owned computers.

Access to the Internet is via the NHS IA provided NHSnet which imposes certain policies which all NHS organisations are required to conform to. Staff using the Internet **MUST** ensure they comply with the **AUP3: Internet & Email Acceptable Use Policy**.

### 4.3.2 Email Access

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

Staff using either the local E-mail service or the National Email & Directory service must ensure they comply with the **AUP3: Internet & Email Acceptable Use Policy**.

### 4.3.3 Rights, Obligations and Responsibilities

Following the IT Shared Services signature to the NHS IA Code of Connection (2002) the IT Shared Services are bound by various Policies, the two most important are;

**SyOP 7.4 – NHSnet: Anti-Virus and Anti-Malware Policy and Procedures – NHS Information Authority. Section 2 Rights and Obligations of NHSnet-Connected Organisations.** Last Modified 06 January 2003.

**SyOp 7.6 NHSnet: Messaging Services – Security \_ NHS Information Authority,** published 06 January 2003

These documents plus more can be found on the NHSnet at;  
<http://www.nhsia.nhs.uk/security/pages/default.asp>

Among the activities that are not permitted while using NHSnet, the following are of particular relevance. Note that the fact that they may take place without the knowledge or intent of the connected organisation or individual, it does not mean that they will be required to take responsibility for them.

- The illegitimate or illegal transmission of any offensive or inappropriate material. Apart from the fact that it's proscribed by policy, it may be associated with the dissemination of malicious code.

- The creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety: this should particularly be noted in the context of forwarding of unverified and/or unauthorised security alerts, chain letters and so on.
- Unauthorised access to systems, data or facilities. This is characteristic of some malicious software: where such software is operating on a connected system.
- Flagrant wasting of staff effort or networked resources. This could be invoked, for instance, where a site or individual persists in forwarding inappropriate mail despite warnings from the NHSIA.
- Processes that result in the corruption or destruction of other users' data or violation of the privacy of other users, or disruption to their work.
- Where NHSnet is being used to access other networks, any abuse of applicable third- party acceptable use policies will be liable to the same measures as unacceptable use of NHSnet.

### **Monitoring Access**

IT Shared Services are responsible for monitoring the access to Internet sites from the NHS organisations. The Head of IT Services (PT & PCTs) is responsible for ensuring that audit tools are available which log by user name and password the sites accessed, the time of day the sites were accessed and for how long, and if a file transfer took place. This information must be made available to NHSnet Security Managers of the NHS Information Authority, on request.

### **Excessive Use**

If there is excessive use of the Internet, the IT Shared Services will notify the Head of IT Services (PT & PCTs) who will raise the issue with the NHS organisations member of staff and their manager.

### **Accessing Offensive Sites**

If an audit trail shows that a member of staff has been accessing a site identified as offensive, the Head of IT Services (PT & PCTs) must be immediately informed. It is the responsibility of the Head of IT Services (PT & PCTs) to inform the NHS organisations Security Officer and an NHSIA NHSnet Security Manager of the security breach. A full enquiry will be undertaken which may result in disciplinary action being taken. When a breach is identified, the access of the person(s) involved will be suspended pending the enquiry conclusion at which point it may be terminated.

### **Reporting on Use**

IT Shared Services will regularly produce an audit report on access to the Internet. This report will be authorised by the Head of IT Services (PT & PCTs) and will be made available to all NHS Operational Managers.

### **Breaches of Security**

All breaches of security or integrity of the network and the associated connections must be disclosed to an NHS Information Authority NHSnet Security Manager as soon as detected.

### **Virus Checking**

The existing computer virus checking policy must be extended to include information received over the network either as e-mail attachments, embedded scripts and applets, or downloaded files. See other sections of this document.

## **4.4 Staff Changes**

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

Before access is given to a User account, the user must complete a Network Use Agreement form. This is given in **Appendix B**.

The Human Resources department will provide a leavers list each month to advise the IT Helpdesk about staff changes affecting computer system access (for example job function changes / leaving department or organisation) so that access rights may be amended or deleted, from effective dates.

## **4.5 Third Part Access**

Third party access to the IT Shared Services network must follow the NHSIA Code of Connection (2002) policy. Refer to <http://nww.nhsia.nhs.uk/security/pages/default.asp>

### **4.5.1 Contractors**

When contractors are employed to assist with development or support of the IT Shared Services computer systems, they **MUST** sign a Confidentiality Agreement before starting work. The Confidentiality form is given in **Appendix C**.

### **4.5.2 Third Party**

Where development or support is outsourced to a Third Party, due consideration should be given to the NHSIA policies relative to this situation in the negotiation of any contract. Refer to <http://nww.nhsia.nhs.uk/security/pages/default.asp>

Each member of the Third Party's staff involved in the development or support task **MUST** sign a Confidentiality Agreement before working on the project. The relevant form is given in **Appendix D**.

## 5. DESKTOP

### 5.1 Use and installation of Software – Licensing

Under no circumstances should software, other than that approved and authorised, be loaded onto NHS organisations computers. Staff must not bring or download software (from the Internet or other computers) onto NHS organisations premises without first getting permission from the IT Shared Services Helpdesk. This includes software downloaded from the Internet for shareware and trial or demo purposes.

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 under the direction of the IT Shared Services Helpdesk.

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

Authorised training software includes "games" shipped as part of MS Windows.

- All proprietary software must be properly licensed for each machine on which it is loaded. Installation media (CD or DVD) to be stored securely for audit and recovery purposes (such as a re-install).
- Copyright software must not be copied without the owner's documented authority, i.e. each software installation copy needs a licence – either individually or a specified site licence.
- Without infringing copyright, a lawful user of a computer program is allowed to make a back-up copy for disaster recovery purposes only.
- Software installations may be audited at any time by either the IT Shared Services or internal/external auditor. Note; this can now be done remotely across the network. Illegally installed software will be reported to senior management and arrangements made to legally licence or delete.
- Copying of proprietary or NHS organisation software onto computers that do not belong to the NHS organisations is in breach of the PT & PCT's information security policy, unless it is for NHS organisational business and authorised by a senior manager. This is still however subject to licensing conditions.

### 5.2 Computer Virus Controls

#### 5.2.1 Definition of a computer virus

A computer virus is a parasitic program capable of independently replicating itself. Viruses attach themselves to other programs on hard disks, diskettes, CD/DVD-ROM's and e-mails. They also can e-mail themselves to others using addresses in the users address book. Some can pass information via e-mail to external sources. All

viruses are harmful, either because they contain instructions that purposely destroy data, slow the system down or cause other kind of damage making the system unstable. More details are included in the IT Shared Services operational procedure **C13: Antivirus & Malware**.

### 5.2.2 Risks

Viruses and associated malicious software can destroy, lock access to, or pass confidential data to a third party. So to protect IT Shared Services data and systems, all users need to be aware of the need for anti-virus measures.

- All of the NHS organisations PC's must run anti-virus software.
- Users should not use computer media that has not been checked for viruses.
- Users should not send computer media to the outside world without checking for viruses.
- Users must contact the IT Helpdesk if a virus incident is suspected.

Further information on the correct handling of E-mails and Internet access are detailed in the document; **AUP3: Internet & Email Acceptable Use Policy**.

### 5.3 Passwords Rules

Passwords have a valuable role in protecting systems from unauthorised access. The user account and password enabling access to the IT Shared Services network are a vital part of security and control access to resources.

Only the person to whom it is issued should use that password. Staff must never divulge a password. They 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 8 characters
- Are a mixture of letters, numbers and symbols
- Are kept secret
- Are not 'VISITOR', 'GUEST' or similar
- Are not shared or written down.

Further expansion on the above plus the rules for access to the network are given in the IT Shared Services operational procedure **C7: Access Control**.

### 5.4 Clear Screen Policy

Workstations require a username and password to be entered before accessing any software on that PC. Windows screen savers with password protection will be used on all PCs with time out set to seven minutes within sensitive locations and a maximum of fifteen minutes at other location.

## **5.5 Personal Use of NHS organisations Systems**

All computer equipment leaving the NHS organisations premises should be authorised by the line manager and a copy of the authorisation should be passed to the IT Helpdesk. Refer to the following Section 6.

## 6. TELE-WORKING/HOME-WORKING

### 6.1 Introduction

Increasingly NHS organisations staff are finding that technology is available to enable them to work out of their office in other NHS organisations sites, at home or elsewhere. This section raises and defines the IT Security issues of this way of working.

The aim of this is to provide staff with information about the standards that must be adhered to when they are using mobile computing facilities, e.g. notebooks, palmtops, laptops and mobile phones, (NHS organisation or privately owned), at home or at other premises.

We want to help staff to take the appropriate security measures during the use and transfer of computer equipment and data when mobile. The security issues covered include physical security of computer equipment, confidentiality of data and implications for the security of the IT Shared Services systems and network. Usage of the NHS organisations computers and data resources must also comply with the organisations legal obligations under the Data Protection Act 1998 and the Copyright, Designs and Patents Act 1988.

If staffs are not sure how to implement the standards in this section, the IT Shared Services team will provide further training and support on request.

### 6.2 Definition of Tele-working

Tele-working in this context is the means by which mobile devices can connect via a telephone link to the IT Shared Services network. This link can be by standard landline using modems or via a digital connection using an ISDN or broadband link and by use of the Mobile phone network providing wireless connectivity.

### 6.3 Definition of Home-working

Home-working in this context is where a staff member has been authorised by the NHS organisation to set up an office at their home. A link to the IT Shared Services network can be by a standard landline using modems or via a digital connection using an ISDN or broadband link. Here we consider Home-working is a similar way of working to someone working on the move.

### 6.4 Definition of Mobile Devices

Mobile devices are those computing devices that in use are not permanently sited or connected to a network.

These include the notebooks/laptops that present an identical look and feel to a desktop PC to the specialist A4 size Tablet types. Also Palmtop devices such as HP Jornada series and various Palm devices from Psion, Compaq and others that can be synchronised with a Desktop PC for calendar updates etc.

### 6.5 Record of Home, Mobile Users

When staffs have obtained the necessary permissions to work from home or use mobile computing devices provided by their NHS organisation, they need to complete the form in

**Appendix E.** This enables the IT Shared Services to hold a record for administrative purposes.

## **6.6 Use of Person Identifiable Data**

### **6.6.1 What is Person Identifiable Data?**

Person identifiable information is recognised as a single or number of items by which a person's identity may be established. These examples are by no means comprehensive:

- Surname
- Forename
- Initials
- Address
- Postcode
- Date of birth
- Other dates (i.e. date of death, diagnosis)
- Sex
- NHS and/or N.I. Number
- Local identifier (i.e. G0 Number)
- Ethnic Group
- Occupation

### **6.6.2 Use of Identifiable Data**

The use of person identifiable data must be notified to the Information Commissioner under the Data Protection Act 1998. Users must notify the Data Protection Officer if they record manual or computerised information to ascertain whether this needs to be notified to the Information Commissioner. Failure to notify is a criminal offence under the act.

### **6.6.3 Formal Authorisation**

Formal authorisation by your line manager is required before person identifiable data files can be taken away from NHS organisations premises. All staff who works with person identifiable data on mobile devices must notify the NHS organisation Data Protection Officer in writing, who will keep a register. The data remains the property and responsibility of the NHS organisation at all times and may not be used for any other purpose other than that notified to the Information Commissioners Office and appropriate in the pursuance of NHS organisation activities.

### **6.6.4 Transfer of Person Identifiable Data Files**

In general Person Identifiable data must not be sent via e-mail. The Information Commissioner has advised that email in general is not secure enough and should not be used to transmit confidential information.

The National NHSemail Contact service has been developed specifically to meet BMA requirements for clinical email between NHS organisations and that it is safe to use for clinical communications, provided BMA guidelines are followed. A copy of the Acceptable Use Policy for the Contact E-mail service is available at: <http://www.nhsia.nhs.uk/AcceptableUse.do>

Note that messages are only encrypted between the NHSemail user and the central NHSemail server and again between the server and the NHSemail recipient. Messages which are sent to non-NHSemail users (even if they are on NHSnet) are not encrypted when they are forwarded by the server. Messages from non-NHSemail users are encrypted by the NHSemail server before being forwarded to a NHSemail recipient.

Note that if you forward a message you receive to another email account, it is treated as a new email and the same rules apply. So if you set an autoforward from your NHSmail account to a local email account, it will not be encrypted after it has left the server. It will not then be safe for clinical communications.

#### **6.6.5 Use of Person Identifiable Data in Public Places**

When you are working in public places - on a mobile computer with Internet access via an Internet Service Provider (ISP e.g. AOL, Freeserve, BT Internet) - you must not have person identifiable data on the computer at any time the computer is connected to the internet as it is unlikely that you will have full security control over it. This is because of the potential for unauthorised access to the computer from the Internet (as advised by the Information Commissioner).

#### **6.6.6 Writing Letters**

You can write letters/reports on mobile devices which refer to persons - using mobile computers with Internet access – but you must store all copies on a removable medium and not on the computer hard drive or other long term memory store. You should not write letters which refer to persons whilst connected to the Internet and any removable medium with such data on should be removed whilst connected.

#### **6.6.7 Removal of Data**

When a NHS organisations mobile device is returned to the borrowing pool or the data is no longer needed the data should be removed from it. Likewise when a mobile device is disposed of or sold on all files need to be removed. The IT Shared Service is able to supply users with software which enables them to delete all data from their PC/Laptop upon request. Please contact the IT Shared Services at Rikenel.

#### **6.6.8 Storage of Confidential Data or Reports**

Mobile devices must be physically protected against theft especially, for example, in cars and other forms of transport, hotel rooms, conference centres and meeting places. This also covers any accompanying files or reports containing confidential data. Agreement must be obtained from your local administrator before these files can be removed from NHS organisations premises.

#### **6.6.9 Use of aggregated data**

You can use aggregated non person identifiable data on mobile devices as the restrictions which apply to person identifiable information do not apply to anonymised data. But if this information is confidential or sensitive you should handle it in the same way as person identifiable data.

#### **6.6.10 Use of Mobile Devices**

Care should be taken when using mobile devices in public places, meeting rooms and other unprotected areas outside of the NHS organisations premises. It is important when using these devices in public places care is taken to avoid the risk of overlooking by unauthorised persons.

#### **6.6.11 Access to Mobile Devices**

To access the mobile device a secure means of password protection and/or cryptographic techniques must be used to avoid unauthorised access to or disclosure of the information stored or processed on the device.

### **6.6.12 Backup of Mobile Devices**

Equipment must be available to enable the quick and easy back-up of information held on the mobile device. These back-ups should be given adequate protection against, e.g., theft or loss of information.

### **6.6.13 Remote access to information**

Remote access to information across public network using mobile devices should only take place after successful identification and authentication, and with suitable access control mechanisms in place.

### **6.6.14 Storage of Equipment**

You should take all reasonable steps to minimise the visibility of mobile devices from outside the home, hotel room, meeting room and to secure windows and doors when the room is unoccupied.

## **6.7 Connection to NHSnet Remotely**

### **6.7.1 What is NHSnet**

NHSnet is a secure wide area network developed exclusively for the NHS. It provides a dedicated NHS network, and a secure and controlled environment for healthcare information. A range of services are supported on NHSnet including: electronic mail, electronic data interchange, access to NHSweb, remote support for clinical systems, access to the Internet, on-line person bookings etc.

### **6.7.2 Code of Connection**

Certain authorised users who remotely access the IT Shared Services network from mobile devices must comply with the Code of Connection to NHSnet and IT Shared Services Network Use Agreement. But this should never take place using equipment that does not belong to the NHS organisations.

### **6.7.3 Internet Access**

Most mobile devices of the laptop variety have the capability to connect to the Internet via their connection to the IT Shared Services network. This connection is still bound by the standard policies agreed to by Individuals as part of their Network Use Agreement.

### **6.7.4 Family Members and Internet Access**

The NHSnet Code of Connection prohibits unauthorised users from accessing the Internet via NHSnet.

## **6.8 Use of Privately owned mobile devices or computers**

General Internet access carries with it a security risk of downloading viruses or programs that can look around a network and infiltrate password security systems. This information can then be sent back to the originator of the program in order to allow them unauthorised access to our systems. The IT Shared Services has security systems to help prevent this happening; however when you use your own mobile device you must exercise care in transferring material between your mobile device and office computer systems. For users that regularly transfer files between mobile devices and work anti-virus scanning software is available from the IT Shared Services. This will need to be updated monthly and users are responsible for ensuring that the update takes place.

### **6.8.1 Virus Scanning of Work**

When you transfer files from your mobile device to the office environment (e.g. via floppy disk or other means) you must virus scan the file prior to using this in your office computer. Contact the IT Shared Services Helpdesk if you are not sure how to do this.

### **6.8.2 Transport and Storage of Equipment**

The local NHS organisations do not carry insurance for the loss of equipment, it is therefore especially important to take care to protect your own or NHS organisation when it is taken off NHS organisations premises.

### **6.8.3 Transport of Equipment and Data or Confidential Documents**

You should take care to minimise the risk of theft or damage. IT equipment must be transported in a secure, clean environment. During transfer of equipment between work and remote work place, you should keep the equipment out of sight and not leave it unattended at any time. Mobile devices and data must not be left in your car.

### **6.8.4 Storage of Equipment**

You should take all reasonable steps to minimise the visibility of mobile devices from outside the home, hotel room, meeting room and to secure windows and doors when the room is unoccupied.

## **6.9 Legal Liability**

There is a legal requirement for the NHS organisations Chief Executive to report any computer crime involving child pornography to the police. Users of the Internet are committing a criminal offence by downloading child pornography and the Trust would be required to involve the police if such material were found on any of its computers.

### **6.9.1 Disposal of paper, media and equipment**

All data must be properly removed from the user's mobile device and any files or equipment returned to the NHS organisation upon termination of employment. The media including the hard disk will continue to hold data even though the relevant files have been deleted. Although a deletion marks the files as deleted, it will only remove the directory entry when releasing space for later use. The actual data can still be read by those who know how. Please ensure that any disks, paper documents are disposed of in a secure way. (E.g. shredded or using the file deletion software supplied by the IT Shared Services.)

## **6.10 Home workers – Health and Safety**

Equipment will only be installed on a home worker's premises where:

- Home worker status has been authorised by HR
- A health and safety check has been carried out

## 7. IT DEPARTMENT

### 7.1 Useful contacts

<b>Name</b>	<b>Position</b>	<b>Base</b>	<b>Tel</b>
Bernie Wood	Head of IT Shared Services (PT & PCTs)	Rikenel	891143
Susan O'Connell	Data Protection Officer	Rikenel	891060
Allan Jones	IT Network Security Manager	Rikenel	891140
Steve Holley	IT Operations Manager	Rikenel	891062
HELP DESK	IT Shared Services Help Desk	Rikenel	891025

**Appendix A:**

**Security Incident Report Form**

**Please return completed forms to:** **Network Security Manager  
Gloucestershire Partnership NHS Trust  
IT Shared Services Montpellier Gloucester GL1 1LY**

<b>Section 1 Organisation Details</b>		
Name	<b>IT Shared Services</b>	Telephone No: 01452 891140
Address	<b>Rikenel Montpellier Gloucester GL1 1LY</b>	Fax No: 01452 891014
Person reporting	.....	
Job Title	.....	
Date of Incident	.....	
Date of Report	.....	
<b>Section 2 System Details</b>		
User	.....	
System Involved	.....	
System Location	.....	
<b>Section 3 Incident Details</b>		
Nature of Incident.....		
Brief Description of incident .....		
.....		
Impact of Incident (Please tick)	Disclosure of Information	<input type="checkbox"/>
	Denial of access to information	<input type="checkbox"/>
	Destruction of Information	<input type="checkbox"/>
	Modification of Information	<input type="checkbox"/>
	None	<input type="checkbox"/>
Significance of incident (Please tick)	Insignificant	<input type="checkbox"/>
	Minor	<input type="checkbox"/>
	Significant	<input type="checkbox"/>
	Major	<input type="checkbox"/>
	Acute	<input type="checkbox"/>
Action taken.....		
.....		
Signature of person reporting incident.....		

## **GUIDANCE NOTES FOR SECURITY INCIDENT REPORT FROM**

### **Section 1 Organisation Details**

Date of Incident :                      Please state date that incident occurred, or the date it was discovered.

### **Section 3 Incident Details:**

Please state the type of incident that occurred, from the list below:

- Hardware damage
- Hardware failure, including environmental equipment
- Hardware theft
- Software failure
- Hacking
- Accidental unauthorised access
- Sharing passwords
- Unauthorised requests for information from unknown sources
- Malicious software, viruses etc. with name
- Human error
- Power failure
- Other - Please specify

Impact of incident :                      Please tick the appropriate consequence of the incident from the list provided on the form.

Significance of Incident :                      Please give an indication of the significance of the incident using the table. Some incidents will have more than one effect, rank according to the most serious

**SIGNIFICANCE MATRIX for Security Incident Report****Significance of Incident**

## Type of Effect

Significance	Organisational Embarrassment	Personal Safety	Personal Privacy	Failure to meet legal or regulatory obligations	Financial loss including recovery costs
Insignificant	Contained within local department or directorate	Minor injury to an individual	Minor distress to an individual	Civil suit or enforcement notice with less than £2k damages/penalty	Up to £10K
Minor	Contained within organisation	Minor injury to several individuals	Distress to an individual	As above , penalties between £2K and £10K	£10K to £100K
Significant	Local public or press aware	Major injury to an individual	Breach of legal or ethical requirements	As above, penalties between £10K and £50K	£100K to £500K
Major	National public or press aware	Major injury to several individuals, death of an individual	Breach as above leading to serious embarrassment of an individual	Penalties of >£50K or custodial sentence	£500K to £1.0 Million
Acute	Questions in parliament	Death of several individuals	As above involving serious embarrassment to a group of individuals	Multiple criminal or civil suits with unlimited costs	>£1.0 Million

**APPENDIX B Network Use Agreement**

I agree to the conditions of use of the IT Shared Services network as detailed in the IT Security Policy and network training documentation.

I understand the security conditions outlined in the aforementioned network documentation concerning physical security of my PC, use of passwords and the importance of virus checking floppy disks in order to safeguard NHS data.

**Please complete using BLOCK CAPITALS.**

<b>Surname</b>			
<b>Preferred Forename</b>		<b>Middle Initials</b>	
<b>Department &amp; Location</b>			
<b>Organisation (PCT etc.)</b>			
<b>Telephone number</b>			
<b>Fixed term termination date (if applicable)</b>			
Email account required?	Yes/No		

<b>Request for Specialist Software/Network Drives</b>				
PAS <input type="checkbox"/>	SUNRISE <input type="checkbox"/>	FINANCE <input type="checkbox"/>	DENTAL <input type="checkbox"/>	OTHER <input type="checkbox"/>

If you are a current or former Gloucestershire NHS employee or are moving from one PCT to another, please complete the following sections:

<b>Former Organisation</b>	
<b>Former email address (if known)</b>	

To help us maintain a secure environment please provide the following information, this will help us to reliably identify you.

<b>Mothers Maiden name</b>	
<b>Favourite Film</b>	
<b>Favourite Holiday destination</b>	

**Access to and use of the NHSnet and INTERNET User Agreement**

- I understand that it is **extremely easy** to import computer viruses and / or malicious programs and that such infection is **very difficult to prevent**. I will therefore at all times exercise the **utmost caution** and to minimise this risk I will ensure:

- That prior to any file download I will be sure that the file(s) to be downloaded are from a reputable source and that I have a genuine NHS Trust business need to undertake the download. If I am unsure about how reputable the download source is I will check this out first before attempting any download.
- That as a minimum, immediately prior to and immediately after downloading (and ideally during) I will run **up to date virus checking software** on my PC to check for software infection.
- I will immediately report to the IT Shared Services Security Person all incidents which might constitute a threat to data security or the network.
- I agree that my access and use of the NHSNet and associated sites will be for NHS Trust business activities only.
- I understand that access and use is granted **on a per user basis** and I will therefore keep my password confidential and secure at all times. I understand that I will be responsible for **all access** gained through my user rights, this includes others who have gained access through them as a result of my negligence even if this is without my knowledge or consent.
- I will abide by the IT Shared Services IT Security Policy and procedures.
- I will not use access to transfer any data that is confidential or patient identifiable.
- I understand that I should not access offensive or pornographic sites or sites not related to work business and that I should not indulge in any behaviour in my access or use that could be constituted as defamatory, offensive or irresponsible, including the sending or distribution of such material.
- I will not make any changes to the access structures set up that enable access to and use of NHSnet and associated sites without the prior approval of the IT Shared Services.
- I understand that at all times that I remain responsible and accountable for my access and use of that access.
- I understand that I **will NOT be able to access ALL network sites**.

**I fully understand ALL the information laid out above and agree that my access to and use of the NHSnet and associated sites will ONLY be undertaken in compliance with the above conditions. Failure to comply may result in disciplinary action:**

Signed.....Name.....

Date.....Dept/Site.....

**Approved by (usually the above persons line manager):**

Signed.....Name.....

Date.....Dept/Site.....

**Your attention is drawn to the following documents; IT Shared Services IT Security Policy, Data Protection Act 1998, Computer Misuse Act 1990 and Copyright, Designs and Patents Act 1988.**

**This section for IT Department use:**

<b>User name</b>										
<b>Date</b>										

**Appendix C Confidentiality Agreement – Contractors**

**IT SHARED SERVICES FOR PT & PCT’S**

**SECURITY OF INFORMATION**

**CONFIDENTIALITY AGREEMENT**

To be completed by persons working in association with the NHS organisation but employed by outside organisations.

In the process of carrying out your duties for and on behalf of NHS organisation, you may have access to confidential information in respect to individual patients and employees.

In relation to this information you are reminded that this information is governed by the Data Protection Act 1998 and unauthorised disclosure of such information is unlawful.

**Declaration**

I agree that I will not disclose to any unauthorised person/s any information which I come in to contact with whilst carrying out my work for NHS organisation.

Signed ..... Name .....

Date ..... Company .....

On Behalf of the NHS organisation

Signed ..... Name .....

Date ..... Position .....

**Appendix D                      Confidentiality Agreement – Third Party**

**IT SHARED SERVICES FOR PT & PCT’S**

**SECURITY OF INFORMATION**

**CONFIDENTIALITY AGREEMENT**

To be completed by persons working in association with the NHS organisation but employed by outside organisations.

In the process of carrying out your duties for and on behalf of NHS organisations, you may have access to confidential information in respect to individual patients and employees.

In relation to this information you are reminded that this information is governed by the Data Protection Act 1998 and unauthorised disclosure of such information is unlawful.

**Declaration**

I agree that I will not disclose to any unauthorised person/s any information which I come in to contact with whilst carrying out my work for NHS organisations

Signed ..... Name .....

Date ..... Company .....

On Behalf of the NHS organisation

Signed ..... Name .....

Date ..... Position .....

**Appendix E**

**IT SHARED SERVICES FOR PT & PCT'S  
MOBILE, HOME COMPUTING & TELE-WORKING**

To be completed by individuals who work using mobile computing devices (either NHS organisation provided devices or privately owned).

In the process of carrying out my duties for and on behalf of NHS Organisations I agree to conform to the Information Security Policy of the IT Shared Services.

Formal authorisation from my line manager is required before person identifiable data files can be taken away from NHS organisations premises.

I must notify the NHS organisation Data Protection Officer in writing, when I work with person identifiable data on mobile/home computing devices.

You are reminded that personal information is governed by the Data Protection Act 1998 and unauthorised disclosure of such information is unlawful.

Form to be completed and returned to the IT Shared Services department at Rikenel.

Signed .....Name.....

Date.....Dept/Site.....

Approved by (usually your line manager)

Signed.....Name.....

Date.....Dept/Site.....