Information Management & Technology Policy

The NHS Walsall CCG SQP approved this statement on:

Date: …March 2013…………………

Signed:
……………………………………………………………………………………………
Chair of the committee

Signed:
……………………………………………………………………………………………
Designated Director

Please note that the exranet version of this document is the only version that is maintained. Any printed versions should therefore be viewed as 'uncontrolled' and may not be the most up-to-date.

The footer must give the title of the document, version control and page of page number.
### Document reference information

<table>
<thead>
<tr>
<th>Version:</th>
<th>1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Ratified</td>
</tr>
<tr>
<td>Strategic Lead responsible</td>
<td>Strategic Lead for Integrated Governance and OD</td>
</tr>
<tr>
<td>Title of originator/author:</td>
<td>Risk and Assurance Manager</td>
</tr>
<tr>
<td>Ratified by:</td>
<td>SQP</td>
</tr>
<tr>
<td>Date ratified:</td>
<td>March 2013</td>
</tr>
<tr>
<td>Date Policy is Effective From</td>
<td>Nov 2011 (previous NHS Walsall Policy)</td>
</tr>
<tr>
<td>Review date:</td>
<td>Dec 2015</td>
</tr>
<tr>
<td>Expiry date:</td>
<td>March 2016</td>
</tr>
<tr>
<td>Date of Equality Impact Assessment</td>
<td></td>
</tr>
<tr>
<td>Target audience:</td>
<td>CCG staff and contractors</td>
</tr>
<tr>
<td>NHS Walsall CCG linked documents</td>
<td>IG suite of documents</td>
</tr>
<tr>
<td>Distribution of the document</td>
<td>Cascaded to staff via email. Information agenda item for team meetings. Available on extranet.</td>
</tr>
</tbody>
</table>

The topics covered in the grey shaded area above can be kept in this table but if the narrative for them is lengthy then it is best if they are put into the main body of the document.
CONTRIBUTION LIST

Key roles involved in developing the document

<table>
<thead>
<tr>
<th>Designation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associate Director of IT</td>
</tr>
<tr>
<td>Risk and Assurance Manager</td>
</tr>
</tbody>
</table>

Circulated to the following for consultation

<table>
<thead>
<tr>
<th>Committee/Group/</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQP</td>
<td></td>
</tr>
</tbody>
</table>

Version Control Summary

Significant or Substantive Changes from Previous Version

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

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Comments on Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0</td>
<td>Mar 2013</td>
<td>Policy ratified</td>
</tr>
</tbody>
</table>

A contents page must be included for documents where the main body of the document is over 3 pages long.
Summary

The purpose of this policy, is to clearly define the permissible and acceptable conditions of use of IM&T systems including the Internet, email and phone systems both landline and mobile by authorised staff in Walsall Clinical Commissioning Group (CCG). This policy also includes use where staff who are not employed by the NHS establishment, but who have authorised access to the above systems through the computers owned or managed by the NHS establishment.

If any user disregards the rules set out in this IM&T Policy, the user will be fully liable and will be subject to disciplinary action by their employing organisation.
1. INTRODUCTION ........................................................................................................9
   1.1. Purpose of Policy .................................................................................................9
   1.2. Statement of Intent .............................................................................................9
   1.3. Scope ...................................................................................................................9
   1.4. Principles ............................................................................................................9
   1.5. Organisational Declaration ...............................................................................9

2. POLICY AIM .........................................................................................................10

3. OBJECTIVES ........................................................................................................10

4. DEFINITIONS / GLOSSARY OF TERMS ...............................................................10

5. ROLES AND RESPONSIBILITIES .......................................................................11
   5.1. Chief Executive ................................................................................................11
   5.2. The IT Operations Manager .............................................................................11
   5.3. The Procedures & Policy Committee ...............................................................11
   5.4. The IT Operations Manager and Deputy ........................................................11
   5.5. Individual Responsibilities ..............................................................................11
   5.6. CCG Responsibilities ......................................................................................12
   5.7. Line Managers Responsibilities .....................................................................12
   5.8. Walsall Informatics IT Services Responsibilities ........................................12

6. IM&T POLICY .....................................................................................................13
   6.1. Job definitions (descriptions) & confidentiality .............................................13
   6.2. Job Descriptions ..............................................................................................13
   6.3. Responsibility for security control of assets & data ......................................15
   6.4. Physical security ..............................................................................................19
   6.5. Removal of ICT Equipment ...........................................................................22
   6.6. Disposal and Destruction of Sensitive Data ..................................................23
   6.7. Secure Disposal of Equipment ......................................................................30
   6.8. Equipment security ..........................................................................................35
   6.9. Computer and network operations ..................................................................40
   6.10. Security incident management ......................................................................45
   6.11. Security implications (procurement and acceptance) ..................................48
   6.12. Protection from malicious illegal software ....................................................50
   6.13. NHS Microsoft Licensing Agreement ...........................................................54
   6.15. Data and software exchange ........................................................................61
   6.16. Policy on the use of electronic mail ...............................................................64
   6.17. Policy on the use of the internet ....................................................................71
6.18. Small IT systems development .................................................................77
6.19. Design and use of spreadsheets ...............................................................79
6.20. Computer and user access control ............................................................83
6.21. Application access control ........................................................................91
6.22. Monitoring system access and use .............................................................92
6.23. Patient information ....................................................................................93
6.24. Data validation ..........................................................................................97
6.25. Data encryption .........................................................................................98
6.27. Business continuity planning .................................................................100
6.28. Compliance ............................................................................................103
6.29. Risk assessment ......................................................................................104
6.30. System planning, procurement and acceptance ........................................105
6.31. Mobile working-Remote Working policy and procedure .......................108
6.32. System Security Policy ...........................................................................112

7. IMPACT ASSESSMENT ..............................................................................116
  7.1. Risk Implications / Risk Assessment ......................................................116

8. LINKS TO OTHER CCG POLICIES ......................................................116

9. LINKS TO EXTERNAL STANDARDS ....................................................116

10. MONITORING, CONTROL AND AUDIT ...........................................118
    10.1. Monitoring .........................................................................................118
    10.2. Reporting ..........................................................................................119
    10.3. Validity of this Policy .......................................................................119

11. BEST PRACTICE, EVIDENCE AND REFERENCES .............................119

12. APPENDICES ..........................................................................................119
    12.1. Appendix A - The data protection act 1998 ........................................119
    12.2. Appendix B - Computer misuse act 1990 ............................................127
    12.3. Appendix C – Classification of Security breaches .............................133
    12.4. Appendix D – Incident Classification Table .......................................134
    12.5. Appendix E – Request for computer Access ......................................136
    12.6. Appendix F - Definitions / Glossary of terms ....................................137
    12.7. Appendix G – Blank .........................................................................138
    12.8. Appendix H – Email disclaimer clause ..............................................139
    12.9. Appendix I – Confidentiality undertaking ..........................................140
    12.10. Appendix J – Good practice in: Mobile Computing .........................148
    12.11. Appendix K – IG SU ..........................................................150
    12.12. Appendix L – Smartcard good practice ............................................176
    12.13. Appendix M - List of external organisations and companies ..........180
12.14. Appendix N  Sample Disposal of Media Record ..................................................182
12.15. Appendix O – Equipment Movement Form .........................................................183
12.16. Appendix P – Computing equipment movement sheet ........................................184
12.17. Appendix Q – Approval for Remote Working .......................................................185
1. INTRODUCTION

1.1. Purpose of Policy

Employers have a duty to document and disseminate to all staff the rules and regulations that are applicable in the use of IT equipment and the input, storing and accessing of data. As a public body we must ensure full compliance with the law as well as protecting patients, CCG and all staff working out of CCG properties whether owned by the CCG or others, from harm or prosecution.

All CCG staff contracts make implicit reference to the adherence of these policies as one of the conditions of employment. Anyone who carries out paid or unpaid work for the CCG and who are not staff of the CCG must sign a temporary CCG contract accepting that they are bound by these IM&T policies.

1.2. Statement of Intent

The CCG will, through the Informatics Directorate, ensure the purpose of the Policy is fulfilled and the Legislative and Common Law requirements are complied with.

1.3. Scope

The policies apply to any CCG staff member who in any way uses or has access to any CCG or any other NHS organisations computer equipment, computer produced information, software / system or network, or anyone who enters data, manipulates data or extracts data on behalf of the CCG.

1.4. Principles

That the CCG adopt best practice with regard to its use of IT that it and its employees act within English law.

1.5. Organisational Declaration

Failure to comply with this policy may result in disciplinary action being taken, which could result in criminal prosecution.
2. POLICY AIM

The aim of this policy is to provide rules and guidelines for the acceptable use of the systems described within.

3. OBJECTIVES

This document:

- Sets out the CCG’s procedure for the protection of the confidentiality, integrity and availability of the systems described within.
- Establishes the CCG’s and user responsibilities for the systems described within.
- Provides reference to documentation relevant to this policy.
- Identifies good practice of what may be transmitted or viewed on systems described within.
- Identifies what activities are forbidden when using email or accessing the Internet.
- Identifies what monitoring the organisation can and will use to identify forbidden use.
- Identifies to users and connected organisations, the CCG’s Procedure and procedures with respect to the monitoring and reporting of Internet, email and phone misuse.

In all cases the user, and in the case of external organisations, the organisation itself, undertakes to understand and comply with the provisions of the following Acts of Parliament:

- Computer Misuse Act 1990
- Human Rights Act 1998
- Criminal Justice and Public Order Act 1994
- Copyright, Designs and Patents Act 1988
- Trade Mark Act 1994
- Data Protection Act 1998
- Interception Of Communications Act 1985
- Common Law Duty of Confidentiality
- Regulation of Investigatory Powers 2000
- Fraud Act 2006

This list is not exhaustive.

4. DEFINITIONS / GLOSSARY OF TERMS

See Appendix F
5. ROLES AND RESPONSIBILITIES

5.1. Chief Executive

The CEO is ultimately responsible for ensuring organizational compliance with all IM&T Policies held by the CCG.

5.2. The IT Operations Manager

The IT Operations Manager is responsible for formulating policy based on the IT industry Best Practice.

5.3. The Procedures & Policy Committee

The procedures & policy committee is responsible for ratifying the IM&T Policies.

5.4. The IT Operations Manager and Deputy

The IT Operations Manager and Deputy are responsible for ensuring the policy is adhered to within the CCG and report to the IT Operations Manager on incidents as outlined in this policy.

5.5. Individual Responsibilities

If any person becomes aware that there has been inappropriate use of equipment, e-mail, phones or the internet they should report it to their line manager, who will inform HR/counter fraud so that the incident can be investigated.

- Users must make themselves familiar with this policy and with the appropriate principles of the laws listed above.
- Users must ensure they are adequately trained to use the Internet, email and phone systems, and if in doubt, seek advice from their line manager as to where to get training.
- Users, in the CCG, in signing their Contract of Employment will be agreeing to abide by the contents of this policy.
- Users will undertake not to wilfully enter any web site which is deemed inappropriate.
- Users will not use email to harass, defame or libel any other person or the CCG.
- Users will not use any social networking sites to harass, defame or libel any other person or the CCG.
- Users must not copy or send to another person any software, image or document which is deemed to be copyright.
• Users will not use the email services (including address book) to undertake any business purpose not connected with the CCG.
• Excessive personal use of Messenger or chat room services is not permitted during working hours.

5.6. CCG Responsibilities

The CCG in supplying the connection to the NHS N3 connection for all staff and connected organisations, needs to ensure that there are no breaches of the NHS N3 Statement of Compliance on the part of any of the connected organisations. Failure to do this could result in the NHS disconnecting the whole of the Walsall Wide Network from the NHS N3 connection. Therefore, the CCG needs to have in place systems to identify breaches and means of taking action against the offending parties.

5.7. Line Managers Responsibilities

• Line Managers will ensure that all of their staff have access to training in the use of the Internet where appropriate.
• Line Managers will take all reasonable steps to ensure that all of their staff who uses the Internet and email are aware of the policies, protocols, procedures and legal obligations relating to the use of Internet. This will be done through induction and mandatory update training.
• Line Managers will ensure all of their staff who use the Internet and email have signed relevant contracts or statements reflecting their understanding of the issues following induction or mandatory training.
• Line Managers will ensure that any inappropriate use will be identified and the user disciplined in line with the CCG policies.

5.8. Walsall Informatics IT Services Responsibilities

The staffs employed within the IT Services department, acting as the delegated agents of the Chief Executive, are responsible for maintaining a safe and secure computing environment in the CCG.

More specifically they are responsible for ensuring that the CCG conforms to the NHS Statement of Compliance and have fully implemented the NHS Security and Access Policy.
6. IM&T POLICY

6.1. Job definitions (descriptions) & confidentiality

<table>
<thead>
<tr>
<th>Objectives</th>
</tr>
</thead>
</table>

To reduce the risks of human error, theft, fraud or misuse of facilities.

To ensure that users are aware of information security threats and concerns, and are equipped to support the CCG IM&T Policies in the course of their normal work.

6.2. Job Descriptions

These should include any general responsibilities for implementing or maintaining IM&T policies as well as any specific responsibilities for the protection of IM&T assets or for particular security processes or activities.

Management should ensure that definitions of job responsibilities, working practices and induction training ensure:

- that IM&T users are, according to their responsibilities, briefed on:
  - IM&T Policies
  - NHS IM&T Security Manual requirements
  - Computer Misuse Act (1990)
  - Data Protection Act (1998)
  - Conduct and disciplinary procedures which may be invoked should a breach of security arise.
  - Freedom of Information Act
• individual accountability

Each member of staff is personally accountable for the function they perform.

• where practicable, segregation of function and separation of duties

• dual control and staff rotation

• documentation of significant work performed

• Sharing of expertise

For critical systems training should be given to at least two people so that if one is absent the activity can be performed by the other.

• individually defined authorities or levels of authority

Each individual should know the extent of his/her own authority.

• restriction of security privileges and access rights to specific job functions

• job responsibilities that do not lead to conflict of interest

It may be necessary to require employees to declare personal interest.

• under existing maintenance contracts "outside" contract staff are required to abide by the same codes of confidentiality as permanent staff.

Generally, management must remain alert to signs that could indicate potential breaches of IM&T security.

6.2.1. Confidentiality Agreement
All staff are bound by the CCGs standard principal statement of terms and conditions of service when they sign their contract of employment. The relevant Confidentiality paragraph states:

“The CCG and its employees have a binding obligation not to release information of a confidential nature concerning patients or staff. Any disclosure, other than to other members of staff and agencies immediately and properly concerned, will be regarded as serious misconduct and will normally result in disciplinary action being taken against you, which may include termination of your employment.”

Agency staff and third party users not covered by an existing contract (containing a similar confidentiality undertaking) must sign a confidentiality agreement prior to connection to organisational IM&T facilities.

When an employee leaves, or there is a significant change of duties, line managers will ensure that:

- the employee is informed in writing that he/she continues to be bound by the above confidentiality agreement.
- passwords are removed or changed to deny access.
- relevant departments are informed of the termination or change, and, where appropriate, the name is removed from authority and access lists.
- reception staff and others responsible for controlling access to restricted areas, are informed of the termination, and are instructed not to admit without permission of Head of Department (or deputy).
- departmental property is returned.

6.3. Responsibility for security control of assets & data

<table>
<thead>
<tr>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>To ensure that the responsibility or the security of all IM&amp;T assets is assigned</td>
</tr>
</tbody>
</table>
It is the responsibility of Directors, Managers and Heads of Departments in consultation with the IM&T Security Officer to nominate the "owner" of specific assets or data within their sphere of responsibility.

6.3.1. Ownership of Assets

An inventory should be drawn up of the major assets associated with each information system. The inventory should clearly identify each asset and its ownership.

Assets include:

- information
- software modules used
- physical assets - PCs, printers, scanners etc
- services

Assets will be identified according to a funded and planned program agreed with the Information Steering Group in accordance with CCG priorities.

6.3.2. Systems Administrator (system manager) - will be responsible for:

- defining and allocating security levels and access rights to individual users.
- data quality
- specifying in security terms what the assets can be used for and who can use them.

6.3.3. System owner (Head of Department) - will be responsible for

- informing the IT Support Department of any changes to the assets in their area of control
• assisting the systems manager in enforcing the secure and appropriate use of the assets

• approving the appropriate security protection for the assets

• ensuring compliance with security controls.

6.3.4. Users of PCs - will be responsible for

• the security of the equipment, software, data that they use

• compliance with other CCG IM&T Policies

6.3.5. IT Operations Manager - will be responsible for

• creating and maintaining a CCG IT Equipment and Software Register (to include brief description, location, serial number (where possible) name of person responsible to keep IT Support Department informed of asset movements.)

• Maintaining record of test dates and results for backup tapes (services) and the dates when routine monitoring tests are due as part of the IT Asset Register (ref. section 2.4.6)

• Maintaining a record of the IT Staff, grade and the systems/services that they are responsible for as part of the Asset Register (ref. section 2.4.6)

• all computer hardware and software maintenance contracts

• agreeing with system managers and heads of department the operational procedures necessary to provide secure information and data quality.

Henceforth, responsibilities commence at initiation of a project.

6.3.6. Systems Administrator (Data Owner) (Systems Manager)
The data owner is responsible for:

- identifying all the data within the area of responsibility.
- specifying how the data can be used.
- agreeing who can access the data, and what type of access each user is allowed.
- determining the classification or sensitivity level(s) of the data.
- periodically reviewing that classification.
- approving appropriate security protection for the data.
- ensuring compliance with security controls in conjunction with IT Operations Manager.
- ensuring compliance, where necessary, with the Data Protection Act (1998), and any other relevant legislation covering personal or medical data.

Patient/personal information sent outside the CCG must be encrypted be labelled appropriately. Only in cases where after a risk assessment has been carried out can data be sent unencrypted.

6.3.7. Segregation of Duties

Each System Administrator is responsible for ensuring that when they grant access to systems they ensure wherever possible that segregation of duties is uppermost in their minds. This is especially important with financial systems or any system where staff with control over input and approval of data could make monetary gain fraudulently.

Where a job function could allow fraud or major theft, the function should be controlled by at least two people, and staff should be rotated on an irregular (unpredictable) basis.
If computer access controls are inadequate to prevent fraud, then paper based or other checks must be implemented to counter the threat.

System Administrators should also be conscious when granting access that staff can through incompetence or malice for example enter patient activity incorrectly which could cause loss of income to CCG, loss/reduction of services, bad media publicity.

Any concerns over segregation of duties should be discussed with system administrators, line managers and the appropriate Director (System Owner)

6.3.8. Clear Desk and Clear Screen Policy

Staff dealing with patient information, have a duty of care to minimise the risk of unauthorised access, loss off and damage to information. They must therefore ensure that they clear their desk of patient identifiable information and ensure that they either log off their PC or ensure the screen saver password is active whenever they are not at work or at lunch, a meeting and the area they work in is not secured.

In addition every effort must be made to position the screen in order to minimise any confidential data being seen by unauthorised personnel.

6.4. Physical security

<table>
<thead>
<tr>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>To prevent unauthorised access, damage and interference to IM&amp;T services.</td>
</tr>
</tbody>
</table>

6.4.1. Physical Security Perimeter

- Advice must be sought from the IT Operations Manager over the security measures which must be deployed to minimise the risk of theft and ensure that confidentiality of data is not compromised. Best practice dictates that no computer equipment to be installed in open areas such as a clinic, or patient waiting area or where patients have unaccompanied access, unless there is an overriding operational reason for so doing. In these circumstances.
• Important or particularly sensitive computer areas must be kept permanently locked or access controlled by locks with codes, which can be changed periodically.

• Staff using computer equipment are responsible for the security of that equipment and must ensure that when unoccupied the door to the room containing the equipment is closed or locked as considered appropriate during the working day and locked at all other times. In secure areas within the organisation or other health establishment this may not be necessary. However, managers are responsible for carrying out a risk assessment leading to an agreed level of security.

6.4.2. Physical Entry Controls

Where an area is designated as a secure area:

• Visitors must be supervised or required to wear a visible authorisation badge.

• All CCG staff must wear visible identification.

Staff have a duty to challenge or report anyone seen interfering with or in possession of computer equipment who is not wearing a CCG identity badge.

In all health establishments, except in places of public access, staff should politely challenge strangers if they are suspicious or concerned about their reason for being in possession of or near IT equipment. If staff, are not happy about the explanation given they should immediately ring the helpdesk if located on the CCG site or the operator/manager in charge at all other locations.

Only those staff whose jobs require it must be allowed to enter areas where CCG computer systems are located.

6.4.3. PC Access security

In order to prevent unauthorised access BIOS passwords will be set by IT Support staff on all PCs or laptops owned or used by the CCG.
Access to all PCs, Laptops will be through Windows authenticated users. This will mean that providing the authorised user has logged off, the PC is switched off or the screen saver is activated; then access will be restricted to authorised users only.

It is the responsibility of every member of staff to ensure that they minimise the risk of unauthorised access to their PC by logging off their PC, when they go to lunch, a meeting, or leave work; or ensure that access to their work area is secured. Where practical, the IT Support Department will only adopt secure authenticated Operating Systems. All new PCs and where possible any installed PC which requires re-building or transferring to another user will be upgraded to latest version of the Operating system that has been validated by the IT department.
6.4.4. Virus and Mobile Code protection software

Virus and mobile code detection software will be loaded onto all PCs and Laptops by IT Support staff in order to detect viruses. Updates will automatically be distributed from a central update server. It may be deemed a disciplinary offence to delete or turn this software off as it could lead to catastrophic consequences for the CCG if a virus was not detected and was to spread around the CCG.

All emails are scanned for viruses, and unauthorised mobile code, on entering or leaving the CCG email server. The software used utilises two different virus detection engines which are automatically updated on a daily basis.

Users must inform the IT Helpdesk of each and every instance of a virus or unauthorised mobile code being detected. Every instance of a virus will be investigated and reported upon by the IT Operations Manager.

6.5. Removal of ICT Equipment

<table>
<thead>
<tr>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure maintenance of records of CCG assets removed from site(s).</td>
</tr>
</tbody>
</table>

All Personal Computers, Laptops, Notebooks, Handheld Computers and associated peripheral equipment, including Monitors, printers and scanners must be authorised for removal from site.

This includes all equipment issued to Home Workers, everyone who works on site who is issued with computing equipment to be used off site and all requests for equipment to be moved internally.

Before any item can be removed from site it must have an Asset Register Number (ASR) entry on the asset register with all relevant details listed including Make, Model and Serial Number.

This effectiveness of this procedure is dependent upon ongoing security checks by Health Informatics and by the managers of all departments to ensure that equipment is not removed from site without appropriate, written authority.

6.5.1. Procedure
1. Completion of the Equipment Movement form in full is mandatory where equipment is moved internally to the organisation. Authority must be given in writing using the form at Appendix O before the equipment is removed from one site to another.

2. The form will be signed and held by Health Informatics until such time as the equipment is returned permanently to Site.

3. Where the removal from site is permanent the form at Computing Equipment Movement Sheet (Appendix P) must be completed for removal of the equipment from the Asset Register prior to the Internal Equipment movement form being authorised for the removal of the equipment from site.

4. Equipment replaced by the manufacturer when sent for repair, must, on receipt, ensure the Asset number is transferred to the new equipment and the asset register updated with the new serial number.

6.6. Disposal and Destruction of Sensitive Data

**Objective**

Outlines the disposal and destruction of sensitive data

6.6.1. Overview of Data Media Types

The following table (Table One) is not an exhaustive list of all possible media types, but instead offers a representative sample of the most common forms of media currently in use. These media types also demonstrate the characteristics that determine the appropriate deletion or destruction methods required to assure data is non-retrievable.

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Data Storage Mechanism</th>
<th>Suggested Removal Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard Disk Drives</td>
<td>Non volatile magnetic</td>
<td>Pattern wiping, Incineration</td>
</tr>
<tr>
<td>CDROM/DVD-R</td>
<td>Write once optical</td>
<td>Abrasion, Incineration</td>
</tr>
<tr>
<td>Media Type</td>
<td>Type</td>
<td>Destruction Method</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>CD-RW/DVD-RW</td>
<td>Write many optical</td>
<td>Abrasion, Incineration</td>
</tr>
<tr>
<td>Magnetic Tape</td>
<td>Non volatile magnetic</td>
<td>Degaussing, Incineration</td>
</tr>
<tr>
<td>Flash Disk Drives</td>
<td>Solid state</td>
<td>Pattern wiping, Physical destruction</td>
</tr>
<tr>
<td>Paper Based</td>
<td>-</td>
<td>Shredding, Incineration</td>
</tr>
</tbody>
</table>

Table One: Media and Data Destruction Methods

6.6.1.1. Non-Volatile Magnetic: Hard Disk Drives

Hard disk drives are extremely popular and are widely used as the primary storage medium for the majority of desktop PCs and laptops. Physically, they can be extremely small while simultaneously providing large amounts of storage space. The storage medium usually consists of a glass platter with a magnetic substrate. Data remains even after removal of power from the drive.

6.6.1.2. Write Once Optical: CDROM and DVD-R

CDROMs and DVD-Rs consist of a plastic platter with an optical substrate applied; a focused laser beam writes the data by ‘burning’ the substrate.

6.6.1.3. Write Many Optical: CD-RW and DVD-RW

Although similar to write once media, write many media uses a light sensitive dye to record the data instead. Laser light changes the state of this dye; this allows the rewriting of the media (although data may not be written sequentially). Due to its low financial cost, destruction is the preferred method of disposal.

6.6.1.4. Solid-State
Solid-state devices usually consist of integrated circuits embedded in a plastic substrate, such as SD memory cards. Storing sensitive information on this type of media is not advisable because of their small size and corresponding ease of loss.

6.6.1.5. Paper Based

Despite the growth of electronic storage, paper based records are still in extensive use. This category may also include other ‘physical’ methods of storage such as microfiche, card and specialist record storage material.

6.6.2. Removal of Data

Many of the methods described in the following sections will be applicable to various different media types. We recommend discussing specific removal methods with vendors/contractors in line with the information provided in this guide.

6.6.2.1. Classification of Data Removal

There are two major data removal classifications that help determine the methods used as well as the possible costs involved, these are clearing and purging.

6.6.2.2. Clearing

If the disk drives/media will remain within the same environment, in which they are currently situated (and existing security measures will continue to cover them), the most appropriate removal method is clearing.

As long as particular sections of data need removing and comprehensive data removal from the media is not required, then non-specialist staff or contractors may carry out clearing.

Typical clearing programs use sequential writes of patterned data, ensuring that data is not easily recovered using standard techniques and programs. The pattern matching should involve at least three writes of data. The following is a typical example:

1st write 01101100

2nd write 10010011
This method attempts to mask any previous data with two sets of data that are a mirror of each other, thus 'blanking' previous data on the disk. A random set of data is utilised to fill all available space with meaningless information.

To ensure that historical data is thoroughly removed it is advisable to make as many passes as is practicable. The likelihood of total data eradication is proportional to the amount of passes.

6.6.2.3. Purging
Purging is required when media moves from an existing security zone to a new security zone. This new zone may or may not be more secure than the current security measures in effect.

After removal of media from its current security context there must be sufficient care taken to ensure that data is irretrievable, even if specialised methods are used (e.g. platter scanning or the use of electron microscopes).

Purging involves the use of more sophisticated tools and therefore requires specialist personnel working within a controlled environment. Advise contractors that purging of the media is required. A minimum of seven passes qualifies as a purging process.

6.6.2.4. Data Removal from Live Systems
There are various scenarios in which data may need removing from a system while still in operation, or reuse of the media is required for financial or policy reasons.

In these cases, make all possible efforts to remove the required data from the target media (while not adversely affecting the performance of live systems or the long-term effectiveness of the media to perform the role required of it). In this case, the most common scenario would be to remove the data from hard disks, or tape backup devices, when a particular application no longer requires it.

6.6.2.5. Data Removal for Media Reuse
Often, media such as hard disk drives are reused rather than completely decommissioned. It is the reuse requirement, therefore, that should be the driving force behind the removal methods used (following the guidance above regarding clearing and purging).
In many infrastructure environments, hard disk reuse is common. A particular disk may be reused across many different individual machines or business uses. In this scenario, clearing is a sufficient method of ensuring data is non-recoverable. Keeping a log of all clearing processes (for each disk drive) provides an audit trail that records all the areas that the disk has been in use and, before reuse of the disk in a different area, the verification of data removal.

Best practice instructs that unless there is a compelling business reason to do so, media should not transfer between differing security contexts. If media does require moving between security contexts, purging needs conducting in line with the guidance (above) to ensure that no data is retrievable, using any means. Maintaining a log (including certificates of verification for each individual media device and information regarding the new use of the disk) is extremely useful as it ensures the media is traceable even after it has left its original security context.

6.6.2.6. Verification of Data Removal

Once a specialist company or contractor has processed the media, there should be a procedure for verification of data removal, including the issuing of certificates.

If local staff have carried out the data removal then the process should be recorded (along with the verification results) and stored with all other relevant documentation.

Tools that attempt to retrieve data from media (which has undergone a data removal process) can be extremely useful in verifying that complete data removal has taken place. If any files or fragments of files are evident, then data removal has been unsuccessful. If so, repeat the process using a greater number of passes or consider using a different technique altogether.

6.6.3. Media Destruction Techniques

Media, which is no longer required (or has passed its effective reuse period), should be passed to a specialist contractor for secure disposal. Many of the techniques described for the destruction of media can involve dangerous substances or exposure to possibly toxic particulate matter, so often require specially controlled environments.

6.6.3.1. Hard Disk Destruction
Due to the current costs of storage, large arrays of hard disks are utilised in preference to other backup methods, e.g. tape. This is due to the ease of retrieval and the added resilience of data when mirrored across many drives.

6.6.3.2. Degaussing
Degaussing is a simple method that permanently destroys all data and disables the drive. Degaussing uses a high-powered magnetic field that permanently destroys data on the platters. It also renders the drive inoperable, requiring manufacturer intervention to replace critical parts.

The recommended specification for data destruction is the SEAP 8500 Type II standard used for classified government material. Equipment that complies with this standard assures complete data destruction.

Degaussing is generally safer than physical destruction and (assuming the contractors use the appropriate techniques) the destruction of data is total and permanent.

The most permanent method is the complete physical destruction of the drive and its platters. Due to the component makeup of disk drives, only a specialist company (in a secured and environmentally isolated location) should carry this out. All casing materials need removing, and the disk platters sanding, to ensure the removal of all magnetic material, prior to the destruction of the platter itself.

6.6.3.3. CD-ROM and DVD Destruction
The construction of plastic media such as CDs makes them particularly vulnerable to damage if handled roughly. Most CDs and DVDs are simply a plastic base with a laser sensitive substrate applied to one side.

Achieving permanent destruction removing this substrate with a machine such as a belt sander may release toxic particulate matter into the atmosphere. It is therefore necessary for professional destruction companies to undertake this type of destruction.

Breaking the plastic base into small fragments, and disposing of the remains as normal waste, is suitable for non-sensitive data. Some paper shredding machines now support destruction of CDs in this manner; follow the manufacturer’s instructions carefully to ensure proper destruction and personal safety.

6.6.3.4. Solid-State Devices
Solid-state devices normally consist of Flash USB drives or memory storage cards for PDAs and other handheld devices. Due to the compact nature of their internal makeup, the complete physical destruction of the device is required to ensure that any recovery of data is impossible.

Incineration will melt both the plastic casing and the internal circuitry of small components such as SD cards. This ensures that it is not possible to reuse any aspect of the internal storage mechanism.

Devices such as USB thumb drives should be physically destroyed using brute force methods. As long as appropriate safety methods are in use, non-specialist staff can destroy these devices. The outer casing requires removal and the internal circuitry needs breaking into tiny fragments (including any integrated circuit chips).

If the device has previously contained sensitive data destruction should be carried out by specialist services and certificates obtained.

6.6.3.5. Magnetic Tape Backup
The most effective method for the destruction of magnetic tape is the disintegration or shredding of the tape media. Physical destruction should take place after the tape is appropriately degaussed.

6.6.3.6. Paper Based
Traditionally, paper based disposal has consisted of simple vertical shredding. However, this method is not suitable for confidential or restricted information.

The UK Security Service (MI5) recommends shredding of paper records be conducted using a cross cut shredder that cuts the paper into pieces of no more than 15mm x 4mm. For further information, see http://www.mi5.gov.uk/output/Page56.html.

Incineration may also be used. However, a certificate of destruction from a specialist contractor is required on completion.

6.6.4. Data Removal and Destruction Management
It is important to maintain an effective method of managing the process of data destruction. This ensures that all media requiring cleaning or destruction is correctly organised and properly audited.
6.6.4.1. Media Log

Use of inventory tracking software may be helpful in limiting the administration overhead in larger organisations. Tracking of hard disk serial numbers should be used a bare minimum for individual component tracking.

The log should also contain a section for destruction or removal certificates; these provide evidence guaranteeing the destruction or sanitisation of the media and the date on which the destruction occurred.

6.7. Secure Disposal of Equipment

<table>
<thead>
<tr>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>To ensure that data and information on electronic media is rendered unreadable or unusable by parties outside the CCG or department of the CCG which owns that data or information when the unit of medium is no longer required.</td>
</tr>
</tbody>
</table>

If a machine has ever been used to process personal data as defined under the Data Protection Act (1998) see APPENDIX A or "in confidence" data, then any storage media should be disposed of only after reliable precautions to destroy the data have been taken (e.g. reformatting disks).

The CCGs current criteria for retention of personal data is 6 years after the subject of the file leaves or becomes 70 years old and for confidential data is as detailed in the document Clinical Records Management Policy under Medical Records sub library in the CCGs Document Library.

Before any storage media are destroyed, disposed of or reformatted, the data on it must be checked to ensure that data that should be moved is not destroyed. The reason is that the vast majority of information we process contains personal data. Under the Data Protection Act 1998 processing includes destruction of data. In the case of the CCG, this can only be done in accordance with the CCGs own data making policies as notified to the Office of the Data Protection Registrar. Any queries should be directed to the IT Operations Manager.
It is essential that ALL such equipment is returned to the IT Support Department prior to disposal.

6.7.1. Disposal of equipment:

Computer hardware disposal can only be authorised by the IT Services who should ensure that data storage devices are purged of sensitive data before disposal or securely destroyed. The procedures for disposal must be documented.

Unusable computer media should be destroyed (e.g. floppy disks, magnetic tapes, CD ROMS).

6.7.2. Media disposal:

All removable media should be reformatted before disposal, however if this is not possible, the media should be destroyed using a magnetic degaussing device or physical destruction.

6.7.3. Disposal Process

6.7.3.1. Overview

The scope of this process covers all current known media types. Some of the forms of media are not used by the CCG so there is no method of disposal; where this is the case the process in this section is marked as “Not Applicable. Medium not used by the CCG”.

To keep the processes as clear as possible and to make adherence easier, wherever possible common methods of disposal will be applied to the various forms of data and information in use.

In these cases cross-reference will be made to the first instance of that method.

6.7.3.2. Classification of data and information

In deciding which method of disposal to adopt it is necessary to classify the data or information that the medium holds into the following categories:

a) data or information that needs to be disposed of securely.

This includes confidential data and information that is covered by the Data Protection Act, personal information, business information, information that could harm the CCG’s reputation or business or interests or those of the NHS, the Department of Health, the wider government or their business partners. (For the rest of this document these items will be called “Secure items”).
b) data or information that does not need to be disposed of securely.

This covers all data or information NOT covered by a) above. (For the rest of this document these items will be called “Non-Secure items”).

If there is ANY doubt as to which category a particular unit of medium falls in then (a) assume above.

Who decides into which category a unit of media falls?

The user or the user-department must decide into which category a particular unit of medium falls. Advice can be obtained from the Information Governance Manager if necessary.

6.7.3.3. The processes

1. Paper documents

Secure items must be shredded, using one of the shredders situated in each of the main sites. Within some sites, confidential waste bins are provided and the routine cleaning process will ensure that the confidential bins are emptied into a secure storage area and then the collected waste paper disposed of by means of an industrial shredder being driven onto site. This is done once the quantity of waste has reached a worthwhile quantity. The shredded material is sent for recycling through the same company.

Non-Secure items can be disposed of either by recycling or through the general waste disposal procedure.

It should be noted that the recycling process does NOT entail shredding before recycling, thus it should not be used for Secure disposal.

The companies used for paper waste disposal are given in Appendix 1 to this document.

2. Voice or other recordings

Secure items:

Tapes from tape-based telephone answering machines and dictation machines should be erased before disposal.

Digital telephone answering machines should have message stores cleared by removing the back-up batteries and unplugging the machine from the mains.

The manufacturer’s instructions should be consulted on how to do this. Once this is done the machine can be passed on to another user or disposed of in the general waste – taking care to follow the environmental policy at the same time.
Non-Secure items can be disposed of either by recycling or through the general waste disposal procedure.

3. **Carbon paper**

   Not Applicable. Medium not used by the CCG

4. **Output reports.**

   These should be disposed of by the appropriate procedure in “Paper documents” in section 1 above.

5. **One-time-use printer ribbons**

   Not Applicable. Medium not used by the CCG.

6. **Magnetic tapes**

   Secure items: all tapes used on IT systems are included in this procedure. All tapes are to be sent to IT Logistics, IT Stores, Jubilee House for erasure of data and disposal.

   Each tape is to have data removed in accordance with the manufacturer’s instructions or the tape has to be totally destroyed by degaussing then physical destruction.

   Once the data has been erased tapes will be disposed of by a 3rd Party Recycling company. See Appendix 1 for details.

   Non-Secure items: be disposed of through the general waste disposal procedure.

7. **Removable disks or cassettes**

   Cassettes: Not Applicable. Medium not used by the CCG.

   Secure items:

   Hard disks should be returned to IT Logistics, IT Stores, Jubilee House, where the data will be removed by a magnetic degaussing machine then by physically destroying the hard drive by 3rd Party company (see Appendix 1).

   Floppy disks and zip disks: these should be either reformatted by the user before disposal or re-use on another system or returned to the IT Logistics, IT Stores, Jubilee House for disposal in the same way as for hard disks in above paragraph.

   Non-Secure items can be disposed of either by recycling or through the general waste disposal procedure.

8. **Optical storage media**

   The CCG uses compact disks (CD) and digital video disks (DVD). Both can contain proprietary software etc. from suppliers and CDs can be written to hold CCG data and information.
At the IT Department:

Secure items:

Re-writeable CDs & DVDs must be re-formatted prior to disposal or re-use.

Read-only CDs & DVDs must be rendered unreadable either by shredding, scratching, heating or similar means which is “bad” for the item.

If sufficient numbers of such disks are to be destroyed then the media should be returned to IT Logistics, IT Stores, Jubilee House to shred the disks.

Once the data has been removed or rendered unreadable as above the disk material can be disposed of via the general waste disposal procedure.

Non-Secure items can be disposed of through the general waste disposal procedure.

9. Program listings

Secure items: should be dealt with as Paper documentation “Secure items”.

Non-Secure items can be disposed of through the general waste disposal procedure.

10. Test data

Secure items: should be dealt with as per the particular type of media’s “Secure items” procedure above.

Non-Secure items can be disposed of through the general waste disposal procedure.

11. System documentation

Secure items: should be dealt with as per the particular type of media’s “Secure items” procedure above.

Non-Secure items can be disposed of through the general waste disposal procedure.

Other data and information

Users with data or information holding media whose disposal is not covered by one of the above processes should be referred to the Information Governance Manager for guidance.

All staff in the CCG have a duty to protect all official information that it is enCCGed with by ministers, the public, and other organisations.

6.7.4. Recording of Disposal
All disposals of media are recorded in the “Media Disposals” record log. This records the date received, the owner, the media type, the number of items, the labelling of items, the date disposed of by the IT Services and who did it. A sample form can be found in Appendix M.

6.8. Equipment security

<table>
<thead>
<tr>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>To prevent loss, damage or compromise of assets and interruption to business activities.</td>
</tr>
</tbody>
</table>

6.8.1. Equipment Location and Protection

All CCG servers will be sited in the CCG Primary computer room a purpose built secure environmentally controlled facility or in the CCGs disaster recovery room, unless there are overwhelming operational reasons for not doing so.

The computer suite has a keypad door entry system and the door into the computer room has a manual keypad door entry lock. The codes to the doors and alarm will be changed annually or in the event of a member of the IT staff leaving the CCGs employ or being suspended form their job.

The disaster recovery room has a manual keypad lock and the corridor to the room also has a manual keypad lock. These door codes will be changed on the same basis as the main computer room.

The computer room is protected by two separate air conditioning systems managed by Skanska. If the thermostat in the computer room linked to the air conditioning units detects a rise in the room temperature outside the tight parameters which have been set or in the event of one failing. Then the secondary unit starts to operate and if both fail a temperature alarm in the computer room linked to the helpdesk monitoring system alerts support staff of the equipment failure. Outside office hours the on-call IT engineer will be notified by the helpdesk support staff in the event of an alarm being raised.

Eating and drinking should be strongly discouraged in areas housing computer equipment.
6.8.2. Power Supplies

The computer room is fed by emergency generator electrical supplies, which feed the UPS units in the computer rooms.

These UPS (un-interruptible power supply) protect all the equipment in the computer room. This is to ensure that critical equipment is protected from power failures or other electrical anomalies.

Elsewhere on the CCG premises a UPS must to be fitted to critical computer equipment to provide protection against power supply fluctuation especially if the equipment is fed from power outlets fed from the generator in the event of power outage.

The communications equipment running the main hospital network is protected by UPS.

Power and telecommunications cabling carrying data or supporting IM&T services will be protected by using conduits, running in ceiling voids, metal ducting etc. as appropriate and practical. All contractors must obey the IEE Rules & Regulations when installing cabling in any of the CCG sites.

6.8.3. Equipment Maintenance

All CCG Servers will be covered by appropriate support and maintenance contracts to be arranged and held by the IT Operations Manager. Where, deemed appropriate support and maintenance arrangements will be entered into for computer equipment (PCs, printers, scanners, and bar-coding equipment). The IT Operations Manager is responsible for all computer related equipment contracts on behalf of the CCG. Contracts entered into will have defined levels of maintenance and minimum levels of performance.

It is the responsibility of IT Support staff to maintain an equipment inventory which identifies all computer related equipment and which identifies whether items are under warranty including period end, whether under a support and maintenance agreement plus period start and end and cost; or whether item is not subject to a maintenance contract.

A record of faults or suspected faults will be maintained via the IT Helpdesk. When a user reports a problem to the IT Helpdesk, IT support staff will assess whether the problem is a user problem or
whether it will require further investigation or reporting to the appropriate maintenance organisation to resolve. The Helpdesk will be responsible thereafter to ensure a satisfactory resolution of the problem.

Where deemed appropriate systems engineers will be escorted and supervised whilst on site.

All support and maintenance suppliers requiring remote access to CCG systems in order that they can carry out their contracted work will come into the CCG over the N3 network or in exceptional circumstances where this is not possible access will be granted via an encrypted VPN link. In both instances access will be confined to the supplier system.

Control of remote access to the CCG will remain with the CCG via Firewall rules.

Where a PC or server hard drive is to be removed from the premises for repair or replacement, it will where possible have the data over written or the Contractor warned of the sensitive data that could be contained on it and their duty of confidentiality.

6.8.4. Security of Equipment Off-Premises

Computer equipment including memory sticks, PCMIA cards, palmtop computers or hard disks which do not form an integral part of the PC/Laptop should not be taken off-site without being encrypted.

Portable computers must be encrypted as they are very vulnerable to theft, loss or unauthorised access when travelling and must not be left unattended in public places. The high incidence of car theft makes it inadvisable to leave computer equipment or media in a car - even in a locked boot.

Staff who have been authorised by their line manager to use encrypted computer equipment outside the CCGs premises have a duty to ensure that the risk of theft and unauthorised access is minimised.

The CCGs membership of the Non-Clinical NHS Risk Pooling Scheme provides cover (in principle) for such equipment temporarily used outside the CCGs premises. However, the cover for damage or theft is subject to an excess of £20,000 per incident. Therefore in practise any loss must be met from departmental/directorate funds.
6.8.5. Computer Asset Register

The IT Support Department will maintain a Computer Equipment Audit database and all IT Support staff have a responsibility to record any new equipment which is installed, moved, or scrapped/stored.

Details of all licensed software which is not included in the Department of Health contract with a number of major software suppliers is also recorded in a software database maintained by the IT Operations Manager all IT Support staff have a responsibility to inform him of any new software which is installed.

In addition the database will contain a record of the tests done on the backup systems (e.g. back up tape recovery tests) and services including a record of the dates done and the planned date for the next routine test.

A record of all the IT staff and the systems that they are responsible for will be included in the asset register together with a record of appropriate training they have been required to do in order to ensure that they can operate, maintain and support users on these systems.

6.8.6. Removable Media

Due to high risk of loss/theft (research has shown that one in four such products are lost or stolen) and inability to secure from unauthorised access of the information contained therein, purchases of the following devices are prohibited.

- Hardware which does not form an integral part of the PC/Laptop
- PCMI card
- USB devices capable of holding information (e.g. memory stick)

The CCGs policy is that only CCG provided encrypted memory sticks can be used with CCG computers. These can be obtained from the IT Department and will be charged to the appropriate departmental budget.

Portable equipment which can be encrypted can be connected to CCG computer equipment, all other portable equipment should not be connected as it may be rendered inoperable. The CCG will not be responsible for any costs relating to unauthorised removed equipment being connected to a CCG PC.
6.8.7. Personal Digital Assistants (PDA)

Only PDAs which have been encrypted by IT support staff are authorised for connection to CCG computer equipment. It is not acceptable to use personal IT equipment for the storage or processing of Patient Identifiable or other NHS sensitive data.

If encrypted PDAs are purchased by the CCG then there use should be restricted to email, diary and contact information and notes only. Patient/staff information must not be kept on PDAs because according to the government’s Office of the Information Commissioner, employers have a duty under the law to protect data on PDAs or similar device, whether or not devices are owned by staff or are bought for them for business use. The responsibility for securing data lies with the company under the seventh principle of the Data Protection Act. A person whose data is inappropriately retrieved if a PDA or similar device is stolen could have the right to claim compensation.

A leaflet given out to staff entitled Good Practice In: Mobile Computing can be found in Appendix J.

6.8.8. Disposal of Patient Identifiable Information

It is the policy of the CCG to ensure that ALL information that may in any way or under any circumstances, possibly be identifiable to a patient is securely destroyed when no longer required.

In the case of paper this should, wherever possible, be shredded. Shredders are located in various departments and wards in the CCG

If this is not possible, the special Confidential Bins, which are destined to be incinerated, should be used.

This is a less secure and more expensive option and should only be used as a last resort.

In the case of computer media and obsolescent computer hardware

The rules are specified in the CCGs IM&T Security Policy (Section 10.6)
• all PCs for disposal which contain hard disks must be returned to the IT Department.

• all hard disks will be reformatted and degaussed or destroyed prior to disposal

• where possible all removable data will be rendered unusable prior to discarding

• all removable storage media no longer require should be returned to IT Department for safe disposal. Details in summary format should be given for each item of storage media returned for disposal.

6.9. Computer and network operations

<table>
<thead>
<tr>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>To ensure the correct and secure operation of computer and network facilities</td>
</tr>
</tbody>
</table>

6.9.1. Network Management

The Local Area Network (LAN), switches, routers, connections and apparatus attached to the LAN and Wide Area Network (WAN and including all aspects of network security are the responsibility of:

6.9.2. Remote Working

Restricted remote access to the CCG LAN and servers is available over the internet via Vpn broadband connection.

Currently access is only allowed from CCG approved and controlled equipment to ensure malicious software is not installed.

Access to the CCG LAN is restricted to approved users who connect via Cisco client software and security fob.

Access has been granted to:

• by exception suppliers for the performance of their duties
• key clinicians to carry out remote clinical work
- IT staff to carry out their support duties
- nominated CCG staff for the performance of their duties

If access is required a call is to be placed with the IT Helpdesk who will send the appropriate forms to be completed.

### 6.9.3. Network Security

- Only IT Support staff are authorised to connect equipment to the LAN or WAN or allow access to the PCT network.

- Only IT Support staff are authorised to install and/or modify any communications software. Measures are available and will be used to detect unauthorised software.

- No dial up modem must be attached to any PC which is connected to the LAN as this compromises network security and breaks the code of connection for the CCG. Only by exception and authorised by the IT Operations manager will PCs be allowed to have a dial-up modem which are remotely accessed by the supplier of a bought in software package. In these instances the modem is only connected to the phone line for the period when the supplier needs to carry out any alterations to their software.

- No access to the Internet is permitted other than that which is provided for via the CCG’s proxy Server. The internet can only be accessed via a Firewall and connections are monitored by URL monitoring software to ensure that banned subject matter is not accessed.

- Access in to and out of the N3 will be through the Firewall as we are contractually obliged as a CCG to ensure that we prevent any unauthorised access to and from the N3 network. Any attempt by CCG staff to access unauthorised systems connected to the N3 network will instantly be picked up by the network carrier who will immediately disconnect the CCG from the network and inform the IT Operations Manager of the incident. An investigation will be immediately instituted and the IM&T Security Officer informed. Serious incidents will lead to disciplinary action being taken.

### 6.9.4. Computer Room access

- Computer room access restricted by a manual button operated lock.

- Access to the computer room is restricted to authorised staff only.
- Codes for entry to the computer room may only be given to the IT staff that have a need to access the room. Similarly, the entry codes to the IT staff office area are to be known only to those who have a need to enter the office on a regular basis as part of their duties.

6.9.5. Documented Operating Procedures

The production and implementation of secure Operating Procedures throughout the CCG on critical/significant computer system lies with the IT Operations Manager.

6.9.5.1. For those systems sited within the Computer room

The IT Engineer responsible for each system will produce a detailed Operational Procedures Manual, which will only be available for access by authorised IT Support staff.

The Operational Policies Manual will cover the following areas:

- a detailed list of all the hardware components, the Operating system and system software, including firmware revision levels, software versions and patch levels
- the details and terms of the support & maintenance cover
- a detailed description of the operational tasks
- details of all interfaces to and from other systems
- the procedures to adopt in the event of data corruption and or loss
- backup procedures
- disaster recovery procedures

6.9.5.2. Changes to Operational procedures

Changes must only be made with the approval of the IT Operations Manager or his authorised deputy.

Such changes will be subject to normal change control rules with a new version number being issued and dated. All versions to be kept in the CCGs document management system with a hard copy being kept in the disaster recovery room.

6.9.5.3. Other corporate systems (not based in the CCG computer room)
The IT Operations Manager is responsible for ensuring that adequate documentation and procedures are in place, which comply with the CCG IM&T Policies, although a Director/Manager/Department Head will be named in the documentation as being responsible for ensuring that the day to day running of the system conforms to the procedures laid down in the Operational Procedures.

6.9.5.4. Network

The network is maintained Skanska as sort of the PFI. IT Operations Manager will ensure detailed plans of the LAN & WAN along with detailed documentation on the configuration of the network equipment is available and up to date. Access to this information will only be available to IT Support staff, maintenance company engineers and auditors.

6.9.6. Separation of Development and Operational Facilities

To reduce the risk of accidental changes or unauthorised access to operational software and business data, where possible the following controls will be implemented:

- new software releases and operational software will, reside in different directories
- system suppliers will be encouraged to maintain a test, train and live environment
- program fixes to operational systems will be applied after testing in the test environment. By exception and after consultation with the It Operations Manager a fix can be applied without testing. We are at this point relying on the suppliers internal procedure.

6.9.7. Security of Third Party Access

Arrangements for third party access to CCG facilities will, as far as is practically possible, be based on a formal contract containing, or referring to, conditions to ensure that the organisation concerned can satisfy the CCGs security requirements. All aspects must be reviewed both in terms of network security and physical security of the computer room and any area used to store personal data (whether in human notable or machine-readable form (i.e. CD or hard disk).

6.9.8. External Facilities Management
This currently applies to the provision of:

- Payroll and Human Resources services and contracts are in place in the form of service level agreements with McKesson for Electronic Staff Record (ESR).
- Integra General ledger and accounts payable services are provided by McKesson.

6.9.9. Capacity Planning

IT Support Department periodically check the disk space used on each of the corporate servers as an aid to predicting extra disk space requirements.
6.10. Security incident management

**Objective**

To ensure that IM&T security breaches are detected, reported and investigated

### 6.10.1. Security Incidents Definition

Any event which has resulted, or could result, in:

- the disclosure of confidential information to any unauthorised individual

- an adverse impact, for example:
  - threat to personal safety or privacy
  - legal obligation or penalty
  - financial loss
  - disruption of activities
  - embarrassment to the CCG
  - any breach of a regulatory obligation of the CCG e.g. Health and Safety, Data Protection, etc.
  - unauthorised access attempted or occurred.

### 6.10.2. Learning from Security Incidents

The IT Operations Manager will monitor the types, volumes and costs of all incidents, malfunctions and will in consultation with relevant managers look to carry out changes to eliminate or minimise the likely re-occurrence of the incident.
6.10.3. Reporting Procedures

6.10.3.1. Duty of users
All users of IT systems and services have a duty to note and report any observed or suspected security weaknesses in, or threats to, systems or services or information indicating a suspected or actual security breach immediately to:

a) their immediate line manager
   or
b) if it involves a superior, to the IM&T Security Officer in confidence
   who will discuss with the SIRO.

Managers or senior members of staff receiving information on an IM&T security incident suspected or otherwise, must report the details as soon as possible to:

   IT OPERATIONS MANAGER, the phone number is available on the intranet

   and follow this up with written details of the incident sent to the Serious Information Risk Owner (SIRO).

6.10.3.2. Process

The IT Operations Manager will:

- Inform the SIRO initially and discuss the actions to be taken
- undertake an investigation of all unusual incidents reported or suspected
- keep a written account of any unusual incidents reported to him either directly or indirectly which do not require a formal investigation.
- Those incidents which are of a serious nature will require the completion of an UTO
form which will be submitted to the Risk Management Department. If the incident is deemed to be significant, major, or acute, it should be reported immediately to the IM&T Security Officer or, in his absence, the Associate Director of IT Services.

- record the results of any investigations in the form of a Completed Investigation Report

- report incidents classified as Significant or above as defined in Appendix C in which the CCG is, or could lead to criminal investigation/charges, adverse publicity to the CCG and or NHS or a major loss of data to the Strategic Health Authority Chief Information Officer and Connecting for Health (CfH) (depending on the nature of the incident and its seriousness)

- pass all records and statements to the risk management department to keep in strictest confidence for future audit.

- report all serious incidents to the IM&T Security Officer either:
  - notifying him of the action taken
  - referring for consideration of further action (e.g. if disciplinary action is likely) and provide:
    - a copy of the completed UTO form, completed Investigation report and any other written material on reports
    - classification of the incident (as defined in Appendix C)

6.10.4. The IM&T Security Officer will:

- report any incidents classified as significant, major or acute to the Associate Director of IT Services and SIRO.

The incident may need to be re-categorised during the course of the investigation.

6.10.5. Security breach by IM&T Security Officer

Any staff member reporting a breach of IM&T security must have unhindered access to the IM&T Security Officer. If the staff member believes the breach is a result of an action or negligence on the part of the IM&T Security Officer, the staff member concerned may contact.

Associate Director of IT Services
6.10.6. Disciplinary Process

The violation of the CCG Security Policies and Procedures shall be dealt with through the formal disciplinary process.

6.10.7. Reporting, managing and investigating Information Governance Serious Untoward Incidents (IG SUI)

All serious untoward incidents that occur in the CCGs will be reported appropriately and handled effectively. The document at APPENDIX J describes the reporting arrangements and the actions that need to be taken in terms of communication and follow up when a serious untoward incident occurs.

The definition of an IG SUI is:

**Any incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals should be considered as serious.**

The above definition applies irrespective of the media involved and includes both loss of electronic media and paper records.

Guidance has been approved by all SHA IG leads and the DH Digital Information Policy Team and is presented as a:-

“Checklist for Reporting, Managing and Investigating IG SUIs V 1-0” (see APPENDIX K)

6.11. Security implications (procurement and acceptance)

<table>
<thead>
<tr>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>To ensure that security is built into systems.</td>
</tr>
</tbody>
</table>
Stand-alone PCs running databases/spreadsheets that are not deemed critical to the CCGs business will be exempt from these regulations, albeit that they may be considered small systems.

6.11.1. Procurement

Procurement procedures must ensure that:

- hardware or software changes which may affect network performance or other operational systems have to be agreed by the IT Operations Manager
- any new IM&T facilities provide an adequate level of security and will not adversely affect existing security
- mandatory and desirable security requirements are included in procurement specifications
- the IT Operations Manager is consulted to ensure that the selected hardware or software will meet the agreed security requirements

The satisfaction of security requirements must be established as part of the procurement process before award of contract. All invitations to tender, responses, notes of meeting, letters, other correspondence and contracts relating to a project must be kept for a period of six years from the date of award of the project.

6.11.2. Security Requirements Specification

Security issues form part of any project's definition. The PRINCE project initiation document (or any alternative project plan) must contain explicit tasks to ensure the preparation of a system security policy and secure operating procedures.

6.11.3. System Security Policy

A written statement of system security policy principles should be incorporated into, or annexed to, the specification for all new or replacement computer systems. Consideration should be given to the need for the final system security policy to comply with the NHS IM&T Security Manual™ recommendations.
As part of the Operational Procedures that IT Support staff produce for each of the corporate systems a section covering the following security standards:

- physical, staff and document security principles
- communications security
- hardware and software security measures
- administrative and procedural security rules

### 6.11.4. System Acceptance

There must be formal documented hand over procedures for the migration of systems from system testing to user acceptance testing. The hand over procedures should contain a section specific to security requirements as approved by the IT Operations Manager.

As part of any contract there must be formal documented user acceptance criteria against which the system can be acceptance tested.

Acceptance testing and approval should ideally be done by users who have not taken part in the procurement. In practice this is rarely possible and for this reason the sign off is the responsibility of the Project Board.

### 6.12. Protection from malicious illegal software

<table>
<thead>
<tr>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>To safeguard the integrity of software and data and to protect the CCG from prosecution and loss of revenue</td>
</tr>
</tbody>
</table>

### 6.12.1. Controls against Malicious Software

- Where staff prepare work (e.g. Word document, Excel spreadsheet, PowerPoint presentation) on PCs not owned by the CCG (e.g. at home) it must only be done if there is up to date Virus and authorised mobile code detection software installed, operational and up to date. The work should be emailed to your work email address where it will be scanned by the email virus and unauthorised mobile code scanner
for maximum virus protection. This work must not include personal/patient information unless evidence is supplied to the IT Operations Manager that they have registered under the Data Protection Act.

- These checks will minimise the risk of virus’s and unauthorised mobile code being introduced into the CCG IT environment. Anti-virus Anti mobile code software is limited in the type of malicious software and mobile codes that it can detect and disinfect. Many of the threats now seen, such as Code Red, Conflickka and Nimda are not simple viruses and worms, and anti virus packages do not always completely reverse their ill effects. Similarly, mobile code such as unauthorised Java codes are often difficult to distinguish from authorised mobile codes.

- The risks to the CCG is real and staff have a duty to ensure that they exercise maximum caution when:
  
  - they receive emails from an unknown source especially if they contain an attachment. If in doubt, delete the suspicious email.
  
  - they receive or are given a floppy or CD from family/friend/acquaintance or the like. Do not load it onto any CCG owned PC.
  
  - Computer publications almost always give away CDs with trial software or shareware do not load any of this onto any CCG owned PC. Not only have these CDs contained viruses but also the software will break licensing laws, is not approved for use within the CCG and may interfere with the running of software the user is required to use as part of the duties.
  
  - Only licensed software registered with the IT Support Department is permitted. It is a disciplinary offence to install or use software which is unlicensed. It is copyright infringement to install and use unauthorised software. Under certain specific circumstances, it may also be a criminal offence. Software for hand held devices will be allowed to be installed on CCG computer equipment where a valid license is produced and with the agreement of the IT Operations Manager. Any illegal copies will be deleted and the incident reported to the IT Operations Manager who will act as described in section 2.6.3
  
  - All software which comes into the CCG must be virus scanned, and checked for unauthorised mobile code, as far as it is possible, even if it comes from the NHS Executive or similar source. It is the responsibility of all staff to ensure that no software is loaded onto a CCG PC until it has been confirmed virus free. IT Services staff hold copies of approved virus scanning software for this purpose and anyone is welcome to bring their disk to the IT Department to have it scanned, or alternatively a call can be tossed onto the IT Helpdesk.
  
  - All PCs must have installed and run CCG approved virus checking software
  
  - Anyone who hears of a virus or unauthorised mobile code warning must inform the IT Operations Manager
Helpdesk. IT Services will then under take to validate the warning prior to issuing a virus or unauthorised mobile code warning by email to as many people as possible as well as putting an article on the CCG Intranet.

- Data or software imported or exported via any network may only be done via the CCG "Firewall" and with the approval of the IT Operations Manager.

- Only software for use in the business of the CCG to be used on CCG PCs

- All computer media that would affect the business of the CCG or its ability to meet its statutory requirements must be "write protected" until a write operation is required

- It is the duty of the individual staff member using a PC to ensure that if it contains personal data then that personal data is processed in accordance with the Data Protection Act (see APPENDIX A).

- The CCGs Director of Information & Performance is responsible for all Data Protection issues and must be informed prior to its use

Malicious software must be reported immediately to the IT Helpdesk. A security incident investigation will be instituted and report produced which may result in disciplinary action being taken.

### 6.12.2. Training and Awareness

- **Training**

  - basic computer skills covering security, backups and write protection etc

  - confidentiality, data protection and computer misuse mandated computerised training courses are provided for all new staff.

  - training, awareness of the obligations of Smartcard users occurs at the time of issuing the smartcards to the appropriately identified and documented individuals in accordance with the latest RA rules. (APPENDIX L)

  - reporting of incidents or suspected incidents and the action to be taken with specific reference to serious untoward incidents (APPENDIX K) will be included in the mandated programme on confidentiality etc.
These are available, and Directors, Managers, Department Heads and Senior Staff are responsible for arranging such training for themselves and any member of their staff who has access to and/or uses computers and confidential or sensitive data.

- **Booking courses, training and awareness sessions**

This can be done by contacting the:

**CCGs training department**

### 6.12.3. Viruses "Disinfection" and removal of Unauthorised Mobile Code

- suspicion of viruses or unauthorised mobile code software on any PC or system must be reported immediately to the:

  **IT Helpdesk**

- Machines affected must be disconnected from the network immediately by simple removal of the network lead (similar to removing a telephone lead) and be switched off

- The machine(s) affected must not be used until cleared to do so by the IT Department which has the necessary software and equipment to "disinfect" the machine and test that it is clear of viruses or other damaging or malicious software.

- IT Support Department, on finding a virus present, will carry out the necessary procedures to disinfect the PC and scan any storage media used on the PC for viruses. A security incident form will be completed.

### 6.12.4. Equipment Used Outside Official Premises

*(ref: APPENDIX J Mobile Computing)*

- must be authorised in writing by the Director/Manager/Department Head responsible.
• the machine must not be connected to any external network without prior approval by the CCG.

• only software approved and licensed by the CCG may be loaded onto CCG equipment.

• such equipment must only be used for the authorised business of the CCG.

• it is not permitted to use any CCG equipment for any paid/unpaid work for any other individual/organisation other than the CCG.

• the employee who is authorised to use this equipment is responsible for its safety, the integrity of the data and for ensuring that NO-ONE else but themselves has access to the machine while it is outside secure, official premises.

• The storing and/or viewing of any type of pornography is a disciplinary offence which will lead to dismissal.

6.13. NHS Microsoft Licensing Agreement

6.13.1. NHS Microsoft Licensing Arrangements 2007 - 2010

This is a three year agreement running until May 2010, during which time the Enterprise Agreement also includes the right to use any new versions of the products included in the agreement. Organisations covered by this EA are licensed for immediate use of all the products included.

6.13.2. What do the new arrangements cover?

The NHS in England has a central licensing arrangement with Microsoft – called an Enterprise Agreement - which provides software licences to all personal computers (including desktops and laptops) for specific core Microsoft products across all of the NHS organisations in England including Primary Care Groups CCGs, Acute, Ambulance, Community and Mental Health CCGs and Strategic Health Authorities, including Special Health Authorities.

The arrangements have been extended to the Department of Health and its relevant authorities. The arrangement also covers Hospices and Palliative Care Units providing care to patients in England and linked to the Hospices Connect Programme.

This is a three year agreement running until May 2010 It includes the right to use any new versions of the products included. The funding for this agreement is provided centrally.
6.13.3. Why are these arrangements better than CCGs purchasing these products with local budget?

By setting up this agreement centrally the NHS negotiated a substantially better price for these products than previously available. This agreement enables speedier progress towards the goals outlined by NHS Connecting for Health (NHS CFH).

Organisations do not need to order licenses for any of these products. A single annual transaction between the NHS and Microsoft replaces the many tens of thousands of individual orders that would otherwise be needed. NHS organisations are immediately covered for legal use of these products.

6.13.4. Who is included?

All NHS organisations in England including

- All Foundation CCGs
- All Primary Care CCGs
- All Acute, Ambulance, Community and Mental Health CCGs
- All Strategic Health Authorities and Special Health Authorities

6.13.5. What software is included?

For desktops and laptops, the following software is included:

Office System 2007 Professional Plus edition which includes

- Microsoft Office Access 2007
- Microsoft Office Excel 2007
- Microsoft Office Outlook 2007 with Business Contact Manager
- Microsoft Office PowerPoint 2007
- Microsoft Office Publisher 2007
- Microsoft Office Word 2007

Office 2007 Step-by-Step Interactive Training

Licensing for Office for Macintosh is also included

Software Assurance on Windows Vista Business (includes Internet Explorer browser)

Core Client Access Licensing which includes:

- Windows Server 2003 CAL
- Exchange 2007 CAL
- SharePoint Portal Server 2003 CAL
- SMS (Systems Management Server) 2003 CAL
- SQL 2005 CAL

(These licenses enable you to have network access to a server running the server version of these products.)
Enterprise Client functionality for these CALs is available, in increasing amounts over the lifetime of the agreement, which will enable organisations to build on the infrastructural benefits gained by fully deploying the core technologies. Microsoft and NHS Connecting for Health are working on a joint Infrastructure optimisation model that will enable organisations to measure the maturity of their software estate and their ability to use the enterprise components of this agreement to their full extent.

Windows 2003 Terminal Services Client Licensing is still available to those organisations who wish to use those licenses – the previous volumes purchased enable those who wish to use TS CALs to do so. You will need to activate them using the previous agreement details. You can obtain these from your Microsoft Account Manager.

6.13.6. What software is not included?

Other desktop products, such as Project and Visio are not included, as they are not being used on every personal computer running Windows in the NHS.

None of the server licenses are included and CCGs should continue to purchase these products via their existing Select agreement.

The Select agreement remains the most cost-effective licensing vehicle for buying Microsoft licensing.

Server products that can be purchased through the Select agreement include:

- Windows Server 2003 – All versions
- Exchange 2007 Server – Standard and Enterprise
- SQL 2005 Server
- SMS (Systems Management Server) 2003 Server
- SharePoint Portal Server 2007
- BizTalk Server 2006
- Internet Security and Acceleration Server 2006
- Microsoft Operations Manager 2005
- Microsoft Identity Integration Server 2003
- Microsoft Business Solutions

This is not a complete list – for details of these and other server products please see [www.microsoft.com/servers](http://www.microsoft.com/servers) or contact the IT Operations Manager.

6.13.7. How do I buy the software that is not included?

The best possible and most suitable pricing available at this time is through the Select Licensing programme. Given the pricing structures in place, you should not purchase any software through the Open Licensing scheme or via the retail channel. A Select enrolment will help organisations manage their license assets and ensure that they receive the appropriate level of support and assistance for their license requirements from Microsoft and their reseller. If you wish to enroll any of your additional server licenses in Software Assurance or subscribe to MSDN, please note that you will need to set up your own Select enrolment. Please note that registered charities have access to the Microsoft Academic License Program.
None of the server licences are included because it is too complicated to try and assess how many servers there currently are and how many new servers are likely to be added in the next three years.

Not all NHS organisations use the email software that Microsoft provides so you must check to find out what you will be using.

BackOffice: All of the BackOffice Client Access Licenses within this agreement are granted the right to downgrade.

6.13.8. Does this agreement cover the licensing for Pocket PCs, PDAs or Palms?

If the handheld device you use is running the Microsoft operating system Windows CE or Windows Mobile then the license for this and all of the core Microsoft software included on it (such as Pocket Word and Pocket Excel) will have been included in the purchase price of your device.

If your device is going to be used as a thin client, accessing services provided by Microsoft server products such as SQL 2005 and provided within the NHS network then you do not need to purchase additional client access licenses. For alternative solutions that access external resources please call the IT Operations Manager.

6.13.9. What is the NHS paying for this agreement?

The NHS is paying a fixed amount per year. The number of devices each year increases to cover an expected growth in the number of users. Microsoft has provided a substantial discount to the NHS based on the volume of devices covered and length of the agreement.


<table>
<thead>
<tr>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>To maintain the integrity and availability of IM&amp;T services and to prevent damage to assets</td>
</tr>
</tbody>
</table>


The IT Support Staff are each allocated a number of servers for which they are responsible for ensuring that the systems are regularly backed up and the back-ups verified and tested.
• back-up procedure and timetable authorised by the IT Operations Manager must be followed

• data on all systems will be backed up each day

• for the majority of systems a set of back-up tapes will be used for each system based on a ten day cycle

• a weekly set of back-up tapes will be used for each system based on a four week cycle

• daily verification that the back-up tape has been successfully written to and data restored to be performed on all critical systems at regular intervals.

• on Microsoft Windows Server 2003 or later servers a daily check of the Event Log, Disc space, Database and tape back-up has completed successfully must be done.

• latest daily and all weekly back-up tapes will be stored, in the fire safe on the CCG site.

• all monthly, and yearly, tapes will be taken and kept within application support.

• all original tapes and master program and operating system media will be stored in the fireproof safe on site within the helpdesk.

• all other back up tapes will be stored in the fire proof safe within application support.

• data recovery will be tested in accordance with IT Computer room operating procedures and the test dates recorded together with the date when the next test is due. These will be recoded in the IT Asset Register for each system. (ref: 2.2.5)

• if live data is corrupt, and there is an indication of the cause it will be corrected before using the back-up data

6.14.1.2. Corporate/Department Systems not run from the Computer room

• back-up procedure, timetable and frequency must be in writing and agreed with the IT Operations Manager
• daily back-ups must be done and the data stored in a location distant from the system and in a place that will offer it a high degree of protection in case of fire or other disaster

• an agreed set of historic back-ups must be kept, together with back-up of operating and program software

• details of back-up and security procedures must be documented in the operating procedure for the system

6.14.1.3. PCs

• where possible PCs will be mapped to a file server where the users data files will be stored.

• otherwise back-ups of important data on PCs should be carried out on a daily basis and the backups kept as secure as possible and preferably in a different office

• training courses and advice are available by contacting the CCG training department.

[NB. Personal data held on computer is subject to the Data Protection Act - reference APPENDIX A]

6.14.2. Fault Logs

All hardware and software faults, or suspected faults, must be reported to the IT Helpdesk and be logged.

The log must contain:

• software or hardware identification

• date, time and description of the fault

All essential media must be re-filed in a safe secure environment after use.

6.14.4. Secure Stationery

All departments must have documented procedures for controlling and handling payment stationery, drugs (or other medical supplies) order forms, and any other stationery having a potential value.


6.14.5.1. All systems must be adequately documented. Documentation must be kept up to date so that it matches the state of the system at all times. Version numbers and dates must be used on all documentation and old documentation must be destroyed to avoid confusion and error. For commercially supplied systems it is the responsibility of the supplier to provide the necessary updates and of the IT Operations Manager to ensure they are distributed appropriately.

6.14.5.2. A copy of the latest documentation must be filed with the IT Operations Manager to ensure that at least one copy is in a safe location.

6.14.5.3. Distribution of system documentation must be formally authorised by the IT Operations Manager and kept to a minimum. A record of who it is issued to must be kept.

6.14.6. Disposal of Media

See also section 6.5.5

- all PCs for disposal which contain hard disks must be returned to the IT Department
- all hard disks will be reformatted and destroyed prior to disposal
- where possible all removable data will be rendered unusable prior to discarding
all removable storage media no longer required should be returned to the IT Department for safe disposal.

6.15. Data and software exchange

Objective
To prevent loss, modification or misuse of data

6.15.1. Escrow Agreements (for critical or sensitive software)

6.15.1.1. A number of Escrow agreements are in place to ensure that the CCG can obtain and continue using operationally critical software in the event of the supplier going out of business (receivership/liquidation etc).

6.15.2. Data Exchange Agreements

6.15.2.1. Safe haven

- A Safe haven policy exists and should be used
- all sensitive data related to patient activity must be sent/received from our Safe haven to Safe havens of other authorised NHS bodies in accordance with EL(92)60
- Safe haven management arrangements are in place in various departments. Contact must be made with the department to establish the correct fax number.
- the data must be sent on separate disks in separate envelopes to reduce the risk of information being identified to a particular patient until it is reconstituted in the authorised receiving Safe haven
- this type of data must be encrypted as a further security measure
- All Common Minimum Data Sets will be sent via the N3 network in accordance with the security rules pertaining

6.15.2.2. Other Data and New Forms/Sets of Data
• the IT Operations Manager is responsible for ensuring formal agreements exist for the exchange of electronic data and software between authorised organisations. Organisations who we have a contract for the supply of IT systems are covered by a confidentiality clause in the contract, however any other organisations we need to send information to must sign a Confidentiality Undertaking Appendix I

• for the CCG the Director of Performance is responsible for making formal agreements for the exchange of manual data between the CCG authorised organisations.

• all other Directors, Managers, Heads of Departments must liaise with one of the above - as appropriate - to ensure that the necessary agreements are in place

• these agreements must specify appropriate security conditions detailed in 2.11.3.

6.15.3. Security of Media in Transit

6.15.3.1. For the submission of commissioning information in line with Caldicott guidelines:

a) to Walsall NHS, GP’s, NHS Community - delivered by our own staff in sealed envelopes or electronically via the Walsall N3 network

b) to health organisations and other PCTs – encrypted and delivered by the Post Office using the first class post or preferably electronically via N3

c) to other hospitals, GPs etc – encrypted and delivered by the Post Office using the first class post, or to local GPs via our own transport or preferably electronically via N3

d) Data sets with patient NHS Number or name and address attached are only permitted to move within the CCG Safe Haven(s). Data sets leaving these Safe Havens must meet the requirements of EL(92)60]

6.15.3.2. Packaging

a) printouts in robust sealed envelopes

b) CDs/tapes in the appropriate protective envelopes
6.15.4. Confidentiality Issue Concerning Used Faxing

6.15.4.1. Receipt and Sending of Faxes

Faxes containing personal identifiable and other confidential information must only be sent to and received by identified and authorised fax machines (fax phone numbers) that are held in authorised Safe Havens (authorisation is by the Data and Information Governance Steering Group)

6.15.4.2. Fax Rolls

In recent years there has been a change within many departments of the CCG away from the use of the older fax machines that have a special roll of white, heat sensitive paper to the newer style of plain paper fax machines that have a cartridge containing a roll of black thermal transfer film to print on plain photocopier paper. The new fax machines provide a much clearer print by melting the wax resin coating on the black film and fusing this onto the plain paper.

It has become evident that many staff, who use the plain paper fax machines are not aware that the black film in the print cartridge retains a clear reverse image of all documents that have been printed. This can be seen as a clear area where the wax resin has been transferred to the paper by the printer. The film roll can be several hundred metres long and will contain hundreds of images of documents, most of which are likely to contain confidential information.

It is essential for all fax machines that:

- They should be sited so that their use can be monitored.
- That anyone attempting to tamper with a fax machine or removing the roll is challenged.
- When the printing film cartridge is removed, the film roll must be placed immediately into a clinical waste (Yellow Bag) for disposal by incineration.
• Used printing film rolls should be disposed of immediately and not stored for later disposal.

6.15.5. Confidentiality and Answer Phones

The CCG advocates the use of its voicemail system with access restricted by a security code to maintain confidentiality of left messages which are often confidential in nature.

If there are overriding reasons to use an answer phone then it is essential that messages being left or played back, that may contain confidential information, cannot be overheard by anyone who is not privileged to have or know the information.

6.16. Policy on the use of electronic mail

Objectives
To safeguard the CCG and its employees from the misuse of email

For the avoidance of doubt, this policy applies to all electronic mail sent or received by or through the CCG IT system.

6.16.1. Email and the law

All users of the CCG email system must be aware that email is not an extension of conversation, to be used as gossip. You must think about what you are writing and then read it carefully as the legislation which applies to paper documentation applies equally to emails. That legislation includes the Data Protection Act 1998, the Freedom of Information Act 2000, and all legislation which prohibits discriminatory acts including the Sex Discrimination Act 1975, the Race Relations Act 1976, the Disability Discrimination Act 1995, the Employment Equality (Sexual Orientation) Regulations 2003 and the Employment Equality (Religion or Belief) Regulations 2003 as well as the laws of libel and copyright.

In a High Court case an insurance company was fined £450,000 because one of its employees had made defamatory statements about its competitor on its internal email system. It is not always necessary to show that any loss has resulted to that person, financial or otherwise. Any statement can be considered to be defamatory if the words, whether expressly or by innuendo tend to lower a persons reputation in the eyes of right-minded people.
• The ease with which email can be sent, received and apparently deleted may
give a false sense of security to many who believe their messages to be
confidential or erased forever.
These assumptions are wrong and it does not take too much effort for prying
eyes to read other peoples email.

• Email is part of the general body of documents created in the ordinary course of
business of the CCG. A “document” can be in any form. Relevant documents
must be disclosed in court and employment tribunal proceedings (including to the
other party) and can also seriously damage the pursuit or defence of a claim in
the courts or employment tribunals, whether relating to the quality of goods or
services, intellectual property rights, discrimination, negligence or otherwise.

• Where email is used to communicate with trading partners and customers, it
must be treated in the same fashion as other forms of business correspondence.
Under the Companies Act of 1985 there are explicit obligations to incorporate
certain information in all business correspondence such as the registered name
and address. This information is required by statute to help authenticate the document.

6.16.2. Email Use Contractual Position
Any use of email by any employee must be in accordance with the terms of the
[CCGs] Policy on Electronic Mail. Any such use must therefore be in agreement and
compliance with these terms as set out in the IM&T Security Policy. Failure to
comply with these terms may result in disciplinary action, which may ultimately lead
to dismissal.

The CCG grants an employee an email account for work related purposes only. The
occasional use for personal mail is not a right and the CCGs takes misuse of email
very seriously.

The CCGs Principal Statement of Terms and Conditions of Service state:
“All documents, emails, records etc., created or received by staff and all other usage
of the CCG's IT facilities, are subject to monitoring by the CCG. There should be no
personal use of e-mail address books or any information acquired or produced by the
CCG. You must familiarize yourself with the CCG's policies on email and internet
use, breach of which may give rise to disciplinary action.”

6.16.3. Confidential Information and Personable Identifiable Data (PID)
It is important to make the recipient aware when confidential information is being sent. This is essential for
any subsequent legal action to be successful in the event of a breach of confidentiality. All emails on a
message–by–message basis should include a notice stating the nature of the information contained within the
message.

Patient identifiable data must not be sent to a personal (non nhs) email address without additional security
such as ‘encryption’. Commercial Internet e-mail services of any sort are not secure and should not be used to
send PID (patient and staff), confidential material or government classified information.
Safe email addresses that do not need material encrypted are those ending as shown below:

****.****@walsall.nhs.uk
****.****@walsallhospitals.nhs.uk
****.****@walsall.gov.uk

PID can only be sent to an ***.***@NHS.Net account from another NHS.Net account unless the email is encrypted prior to leaving the CCG network.

If it is necessary to send patient identifiable information by email (via N3), this is (ONLY via the NHS network - N3) acceptable providing that great care is exercised in selecting the correct recipient and the minimum number of patient identifiers are used i.e. NHS Number and D.O.B. Any communication that could materially affect a patient’s treatment must be kept as part of the patients notes. Emails of this nature must not be sent via the Internet.

The confidentiality clause is not automatically inserted by Microsoft Exchange on email sent externally. The wording of a disclaimer is given in APPENDIX H.

6.16.4. Auto Forwarding

Staff must not automatically forward their e-mail to a commercial ISP (Internet Service Provider) such as Hotmail or Google mail to enable access at home.

6.16.5. Misuse of email
Any employee who abuses the use of the CCGs email system through any of the following:

- Personal email is defined as anything that is not directly to do with a work matter. This includes words, images and files.
- excessive personal use (defined as sending more than five emails on any day) or sending emails constituting in excess of 500 words in aggregate in any one day;
- use of your work email account to receive personal mail is only allowed on an infrequent basis. All personal email should be read and deleted once read. Any correspondence/images received of a obscene, offensive, pornographic or damaging nature to the CCGs reputation or which may be considered by others to
cause distress, harassment or discrimination must be instantly deleted. The sender must be warned that you do not wish to receive email from them. If further email of a similar nature continues please inform the IT Operations Manager who will prevent further receipt of emails into the CCG from this source.

- the storing of emails, images, files sent or received by email which are deemed to be obscene, offensive, pornographic or damaging to the CCGs reputation or which may be considered by others to cause distress, harassment or discrimination will result in suspension and likely lead to dismissal:
  - sending email internally or externally which may damage the reputation of the CCG
  - sending email which discloses personal data regarding another individual in breach of the provisions of the Data Protection Act 1998;
  - sending email which constitutes "junk" email or is posted to multiple news groups
  - conducting any private business or commercial transaction using the email system
  - inviting mailback, response forms or orders to the CCG
  - sending email containing libellous or defamatory remarks
  - sending email which is obscene, offensive, pornographic or damaging or which may be considered by others to cause distress, harassment or discrimination on any prohibited grounds
  - using the email system to bully, harass or victimise another employee;
  - using the email system for illegal purposes;
  - using the email system to transmit computer viruses whether knowingly, recklessly or carelessly, will be subject to disciplinary action including the possibility of dismissal inline with CCG disciplinary policy.

The above provisions apply equally to any attachments, images or internet links sent by email.

### 6.16.6. Monitoring and/or interception of email

In order to ensure that the IT system is not used for fraudulent, illegal or any other unauthorised purpose the CCG reserves the right to monitor and/or intercept emails. Where possible, monitoring may be automated to reduce the possibility of monitoring personal emails but there may be circumstances in which this is not possible.

The IT Operations Manager has the authority to permit monitoring of emails whenever he considers there are reasonable grounds to do so. You should assume that any email communication you send can be monitored and accordingly you do not have any reasonable expectation of privacy in this regard.

The IT Operations Manager may also authorise the interception of emails in the course of their transmission for the following reasons:

- to establish the existence of facts;
- to ascertain compliance with regulatory or self regulatory practices and procedures;
- ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system;
• prevention or detection of crime;
• investigating or detecting unauthorised use of the system; and
• ensuring the effective operation of the system.

The CCG requires access to employee’s emails for the following reasons:

• In the event of a member of staff being absent from work for any reason and their line manager requests by email to the IT Helpdesk that they be granted access to the absent staff’s email, then access will be granted in order to ensure the CCG can continue to carry out its business and to determine whether any email communications received by an absent employee are relevant to the business. Email users may also nominate a deputy to action emails on their behalf in the event of any absences from work. The email user will be able to set up different permissions, which include reading through to creating, editing and actioning dependant on the users wishes;

• If a member of staff suspects another member of staff of impropriety, on the Chief Executive, Directors or Assistant Directors authorisation either another member of staff or usually the IT Operations Manager with assistance from his technical staff will go through the entire mailbox of the suspected member of staff un-deleting any relevant emails. Emails felt to be relevant to any investigation will be printed off as potential evidence in any subsequent disciplinary or criminal case. If any other members of staff are suspected of involvement then their email will also be read and kept as evidence in the same way;

• If it is suspected that a member of staff is using the CCG email system in any way that contravenes the CCGs IM&T Security Polices or is in breach of CCG Standing Orders, then after authorisation from the Chief Executive or Director or Assistant Directors, the suspected staff members email account may be de-activated and the emails read in order to gather evidence for subsequent disciplinary or criminal action; and

• If concern is expressed from other staff or a manager about any member of staff who negotiates for the purchase of goods or services, then on authorisation from the Chief Executive or Director or Assistant Directors, they can have their email read to check that the content does not affect any agreed purchase or contract conditions.

It is an implicit condition of the use of the IT system that consent to this monitoring and interception is given.

The only way to avoid personal mail from being monitored or intercepted as set out above is to not use the CCG email system for non work related matters.

6.16.7. Code of Conduct for email usage

• Emails should be related to CCG business and usually sent to an individual or a limited number of people. Occasional private usage is permitted providing that the messages are kept short and infrequent (in accordance with the above guidance), and do not contravene any laws or constitute an unauthorised use of the system. Please be aware that if you do not want personal email to be monitored then do not use the CCG IT system. Marking personal emails ‘private’ will assist the IT Department in avoiding the monitoring or interception of personal emails where possible. Personal emails should also have the ‘signature’ section removed, as you
will not be writing them in a professional capacity. However, the CCG reserves the right to monitor and, where necessary, intercept emails marked personal/private.

- Think before you send an email, and never email rashly or in anger.
- Make sure emails are clear and not open to misinterpretation.
- Use email efficiently to avoid unnecessary work for others. Sending copies should be strictly limited to those to which it directly effects. Research has shown that the vast majority of emails copied to multiple people are never read.
- “Flame mail” is email that is abusive, aggressive or deliberately anti-social is strictly forbidden. This includes messages that are harassing, upsetting, insulting, rude, obscene, sexually explicit or unduly sarcastic. Remarks sent by email that are capable of amounting to discrimination including harassment under the Sex or Disability Discrimination Acts, the Race Relations Act, the Employment Equality (Sexual Orientation) Regulations or the Employment Equality (Religion or Belief) Regulations or any other relevant legislation prohibiting discrimination could lead to complaints and/or employment tribunal claims against the CCG and against the employee sending the email. In such circumstances the CCG may take disciplinary action up to and including dismissal.
- All instances should immediately be reported to your line manager and to the IT Operations Manager for investigation.
- Email should not be used to manage people or to avoid face to face communication or difficult matters.
- Don’t use email unless you need to share documents or need written documentation of your message.
- Remember to select the correct email address you want your message to go to.
- It is strictly forbidden to send patient identifiable information over the Internet as it is not a secure medium. However, it is acceptable to send such information over the Walsall N3 network.
- The ease of use of email can lead to unguarded and impetuous comments being made, which in turn could be classified as defamatory. Defamation arises where there is the publication of an untrue statement tending to lower the subject of the statement (which may be an individual or an organisation) in the estimation of the public generally. Liability for the tort of defamation applies to electronic communication just as it does to more traditional forms of publishing. You are therefore advised to take care when drafting emails to ensure that the content is not libellous.
- Care should be taken when sending file attachments as these are typically large and may cause network congestion. File attachments should only be sent when necessary and should be deleted as soon as is practicable. The maximum permitted size for internal and external attachments (whether sent or received) is 10MB. This is to prevent viruses and other undesirable programs, software or files being received or transmitted.

6.16.8. Communications with External Bodies

- Only those CCG employees who are duly authorised to speak to the media, to analysts or to the public on behalf of the CCG may do so via email.
- Other employees may participate in email correspondence only if they explicitly state that they are expressing a personal viewpoint and not that of the CCG external emails must make clear whether the message contains the views of the individual or of the CCG.
6.16.9. Information for Email Users

- Email users should be cautious about email attachments from people or companies you do know and you should not believe them to be safe even though you know the sender.
- Worms generally spread by sending themselves without the knowledge of the person whose account they spread from. If in doubt, delete the attachment. One recent incident involved a virus which sent out an email saying that a safe attachment was on its way, and then sent out a copy of itself as an attachment. Bear in mind that even a legitimate, expected attachment can be virus infected; worms and viruses are related, but slightly different problems.
- Regard anything that meets the following criteria with particular suspicion:
  - If they come from someone you don’t know, who has no legitimate reason to send them to you;
  - If an attachment arrives with an empty message;
  - If there is some text in the message, but it doesn’t mention the attachment;
  - If there is a message, but it doesn’t make sense;
  - If there is a message, but it seems uncharacteristic of the sender either in content or in the way it is expressed;
  - If it concerns unusual material like pornographic web-sites, erotic pictures and so on;
  - If the message doesn’t include any personal references at all (for instance a short message that just says something like “You must take a look at this” or “I’m sending you this because I need your advice); and
  - You are strongly advised that they think carefully about giving their email address to any internet site which is not an NHS site or CCGed site. Once organisations have your email address they commonly will sell it on to other organisations. This leads to often large amounts of unsolicited and unwanted (i.e. pornographic) emails being sent to you.

6.16.10. Etiquette

The following should be observed:

- All email messages should be written in lower case as using CAPITAL letters is considered to be aggressive.
- The subject field should always be used to add a short description of the contents of the e-mail. This will assist the recipient in prioritising opening of the e-mail and aids future retrieval of opened messages.
- Care should be taken with content. Nothing should be written in an e-mail that would not be written in a letter or said to someone face to face.
- The same conventions should be used as when sending a letter by post, e.g. using the same style of salutation.
- External emails should be signed with the name, title and contact details of the sender. This can be added to a signature file so that it appears automatically by following the steps outlined below:
  - select the Tools menu from the menu bar in your Inbox;
  - then select Options;
  - then select the Mail Format tab; and
  - add a signature file by using the Signature Picker.
6.16.11. Formation of Contracts

Under English law the vast majority of commercial contracts can be established in any form chosen by the parties, whether in writing, orally or through an exchange of emails. E-mail is capable of forming or varying a contract in just the same way as a written letter.

Such a capability gives rise to the danger of employees inadvertently forming contracts on behalf of the CCG varying contractual terms to which the CCG then become bound. All email users must be aware that emails sent to a supplier during contract negotiations may form a collateral contract even though the final written contract explicitly excludes such representations.

Staff should take care when drafting the words of an e-mail so that they cannot be construed as forming or varying a contract when this is not the intention.

Email users must be aware that they must not circumvent the CCGs Standing Orders on the purchase of goods and services by the use of email.

6.16.12. Housekeeping

It is necessary for you to determine which emails are work-related and are to be archived and which emails are personal and be deleted.

**Work-related emails** should be retained and archived if required to your Personal Folders.

**Personal emails** retained in the personal Inbox should be kept to a minimum.

6.17. Policy on the use of the internet

**Objectives**

To safeguard the CCG and its employees from the misuse of the Internet

6.17.1. The Internet and the law
The Internet is an uncontrolled, unmanaged and largely unsupported world wide network of computers, however although the Internet covers the world, domestic law applies to access made in this country and all users must ensure that they are aware of and comply with all relevant laws.

- In essence the principles of general law and legislation that apply to paper based information apply equally to the Internet. This legislation includes the Data Protection Acts 1998, The Sex Discrimination Act and the Race Relations Act.

- In addition the law of computer misuse and forced/unauthorised access to computer systems also applies to the internet (The Computer Misuse Act 1990) (APPENDIX B)

- Any copying from the Internet must be with the permission of the copyright owner, otherwise a breach of copyright law may have occurred. Unauthorised copying and distribution of computer software is always copyright infringement.

- When communicating over the Internet you must not make unpleasant or derogatory remarks or imply them about a person, otherwise this can lead to libel action, for which the CCG can be liable as well as you.

- Receiving or downloading of information or data, the existence of which contravenes national legislation is regarded as system misuse.

- The distribution (or possession with a view to distribution) of pornography, other offensive material could result in the CCG being prosecuted for failing to take satisfactory measures to prevent the breach of national legislation. Significant damage to the CCGs reputation would then follow from the adverse publicity associated with such a breach.

The Internet is not secure and caution should be exercised over its use especially over the information that you provide either about yourself or the CCG.

Although the Internet contains a wealth of information, the accuracy of the information available over it must not be relied upon as anyone in the world can publish what he or she want. The Internet also contains a wide array of sites that contain information, which is non work related and in some cases which breaks domestic law.

All existing CCG policies apply to the use of the Internet, particularly those that deal with patient information and data security, confidentiality and copyright.
6.17.2. Internet Use Contractual Position

CCG Principal Statement of Terms and Conditions of Service state:

“Any use of the CCG Intranet and access to the Internet must be in accordance with the terms of the CCG Policy on the use of the Internet. Any such use must therefore be in agreement and compliance with these terms as set out in the IM&T Security Policy. Failure to comply with these terms may result in disciplinary action, which may ultimately lead to dismissal.”

6.17.3. Internet Access

6.17.3.1. Access

Internet access is not a right and is provided primarily for work related use. Access to the internet is only granted to staff subject to the following restrictions.

Use for purposes other than those which are work related, is a with-drawable privilege. Any such use must not interfere with the user’s duties or those of any other user. Nor shall the internet or email used in any way that brings the reputation of the connected organisations or the CCG into disrepute.

Access to inappropriate material is strictly forbidden, e.g. pornography, instruction on criminal or terrorist skills, promotion of cults, gambling, content or statements of a nature, which are liable to cause offence to others, or any other material likely to bring the CCG into dispute.

The CCG runs software which has classified around 1.5 million websites into categories such as Health Related, Sport etc. In order to protect the CCG from possible prosecution it prevents access to sites which have been classified as:

- Adult/Sexually Explicit
- Advertisements and Pop-Ups
- Gambling
- Glamour and Intimate Apparel
- Intolerance & Hate
- Criminal Activity
- Violence
- Weapons
- Illegal Drugs
- Hacking
• Spam
• Spyware
• Social networking sites
• Chat
• MSN Messenger
• Yahoo Messenger
• Streaming Media (video & radio)
• This list is not exhaustive and will be subject to change

Anyone found trying to circumvent the CCG's URL blocking software by the use of proxy avoidance web sites or any other method will be subject to disciplinary action.

Public Proxy websites include but not restricted to:

Publixproxyservers.com
Proxyway.com
My-proxy.com

Software is constantly monitoring by user sites which are being accessed, anyone trying to access any of the above classes will be prevented by the software and a log kept of the transgression. Serial offenders will be reported to their line manager and or head of department.

Access to the Internet may be used for any legal activity that is in the furtherance of the aims and policies of the CCG. Internet access should be primarily for education related purposes, to research relevant topics and to obtain useful health service information. The CCG is not licensed to provide commercial services through its Internet provider.

6.17.3.2. Unintentional breaches of security

If inappropriate material is inadvertently viewed by mistake operate the ‘Back’ button immediately and inform your line manager. Downloading of such material may constitute an act of gross misconduct. However the CCG notes that access to subjects and sites of a potentially contentious nature may be appropriate in some areas of normal operation and/or in specific circumstances, e.g. sex education youth advice, counselling on gambling, approved research, etc. The CCG therefore places special responsibilities of care on staff operating in such areas to ensure that such access is necessary and that other users, staff and members of the community are not exposed to any such material without good cause.
6.17.3.3. Allowable use

A small limited amount of personnel Internet browsing by CCG staff is allowed at lunch or break times, providing it does not breach any CCG IM&T policies. **Please be aware that this usage is monitored.**

Users are allowed to use the Internet and email for limited personal use providing none of the “Unacceptable Usage” rules are contravened (see below). Personal use is at the discretion of the CCG and individual Line Managers. If demands at particular times of the day become excessive (i.e. lunchtime etc), and performance of the network suffers as a result, personal use may have to curtailed.

6.17.3.4. Acceptable Usage

- To access research material and other information relevant to your work.
- To access web sites and web mail accounts for personal use so long as this does not interfere with work, or the work environment, and if it does not breach locally defined policies and practices. This should be done in the users own time, i.e. before shift, during breaks or after shift.

6.17.3.5. Unacceptable Usage (this list is not exhaustive)

- Creating, downloading or transmitting (other than for properly authorised and lawful research) any obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- Creating, downloading or transmitting (other than for properly authorised and lawful research) any defamatory, sexist, racist, offensive or otherwise unlawful images, data or other material.
- Creating, downloading or transmitting information of a terrorist content that would otherwise draw the attention of security agencies to accesses made from the organisation.
- Creating, downloading or transmitting information of a criminal nature.
- Creating, downloading or transmitting material that is designed to annoy, harass, bully, inconvenience or cause needless anxiety to other people.
- Creating or transmitting, or forwarding “junk-mail” or “spam”. This means unsolicited commercial webmail, chain letters or advertisements.
- Using the Internet to conduct private or freelance business including the provision of Private Healthcare) for the purpose of commercial gain.
- Creating, downloading or transmitting data or material that is created for the purpose of corrupting or destroying other user’s data or hardware.
- Downloading streaming video or audio (e.g. Internet Radio) for entertainment purposes.
- Excessive access and responding to personal emails during working time.
- Using the email system and in particular the CCG and NHS address books for the purposes of conducting business unconnected with the CCG and the NHS.
- Accessing or using Public Proxy sites.
- Accessing Social Networking Websites.
- Creating, downloading or transmitting data or material for fraudulent use.
- Excessive use for non-work related purposes.
If the volume of activity over the link to N3 causes this link to become unacceptably slow then the IT Operations Manager will give priority of access to the business of the CCG to ensure that it can continue (i.e. payroll, purchasing of supplies etc). This may mean restricting or even preventing access to internet users during this period.

Access to the Internet by Medical staff using the CCG Library PCs is for medical research and educational purposes only.

No dial-up access to the Internet is allowed from CCG property, access must be made via the secure CCG N3 high speed digital connection.

The IT Support Department will record all Internet traffic and will intermittently monitor Internet usage to deter inappropriate use or in cases where abuse of the system is suspected. The police will be involved in all appropriate cases, including those of child pornography being accessed/stored on any computer or kept in paper form on CCG premises.

No pornographic or obscene images or documents of a pornographic or obscene nature must be stored on any computer on CCG property or transmitted across the CCGs' LAN. Any instance will give grounds for instant dismissal.

Anyone attempting to access information which may be deemed to be linked to terrorism in any way will be reported to the police.

6.17.4. Downloading Software / Files

Great care should be exercised in downloading files from the Internet as there is a high chance that they may contain a virus, which could not only affect an individual PC but PCs throughout the CCG.

All programs downloaded from the Internet must be relevant to the individual work, must be fully licensed and registered with the IT Operations Manager. Unauthorised copying of software and failure to comply with the correct licensing of software is copyright infringement and a disciplinary offence.

Downloading, of non standard software (i.e. Kazaar), file sharing software such as utorrent and WIN MX, customisation software such as hotbar is strictly prohibited.
Shareware programs are subject to copyright laws and are not free they still must be purchased and licensed. Failure to comply could render the individual and/or the CCG liable to substantial damages and legal costs.

- The CCG policy is to purchase all software centrally from an approved list of software and any programs downloaded from the Internet must whether purchased or free, still be approved by the IT Operations Manager before being used.

- If large files or programs are to be downloaded or printed it is recommended that the downloading commence after normal business hours thus reducing the possibility of network traffic congestion.

6.17.5. Streaming Media

Unless there is a clinical reason for someone require streaming media (video, radio, TV) access will be denied by Internet filtering software in order to provide reasonable response times to all users.

6.17.6. Social Networking Sites

Access to all social networking sites during work time is banned whether or not access is available or not.

6.18. Small IT systems development

<table>
<thead>
<tr>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>develop systems in a consistent and supportable way ensuring that the investment in Corporate systems is maximised</td>
</tr>
</tbody>
</table>

Introduction

Historically, due to a lack of investment in IT and no clear strategy, it became the norm for staff with an interest in computers to spend considerable amounts of time developing small computer information systems.
These systems were written utilising different database packages, were undocumented and were more often than not unsupported after their initial writing. This situation resulted in no assessment of need or benefits, experienced staff being diverted from their primary role (often for long periods), no system documentation and support for the system only being available from the individual involved.

For those reasons and to bring such developments within the CCGs IT Strategy the following policy is in place:

**Process**

- Proposer to identify information requirements
- Discuss requirement with IT Operations Manager (who will advise on the best way of addressing the need within the CCG Strategy).
- Proposer to formally document their requirement and complete an Informatics pro-forma. (in order to ensure that there is no misunderstanding of needs).
- Informatics will then investigate, in consultation with the proposer, the preferred approach to deliver the identified need in the following order.

1. Will one of the Corporate Systems provide the solution?

2. Will a small development on a corporate system by IT Support staff or our software suppliers provide the solution?

3. Will a package provided by external supplier provide the answer?

4. In exceptional circumstances a system will be written, usually by Informatics using the prevailing CCG standard database.
a) A detailed system specification will be produced and agreed with the user.
b) Documentation covering system design will be provided.
c) User Manual will be provided.

- All small system development undertaken must be supportable by the CCG IT Services Team, fit within the CCG IT Strategy and the CCGs IM&T Policies.

- Any system, either "free standing" or that may require to be linked to the Local Area Network and/or the NHS Network, must be approved as meeting the necessary security criteria by the IM&T Security Officer appointed by the CCG (HSG(96)15).

The intellectual property rights in all computer programs, databases and their associated user and systems documentation which are written by an individual employee in the course of his or her duties, whether or not CCG assets are used will belong to the CCG. It is a condition of your employment that you agree, on request, to sign any document reasonably required by the CCG to establish or confirm its ownership of their intellectual property rights.

N.B. Small IT Systems does NOT include large Microsoft Word processing/Microsoft Excel Spreadsheet documents or macros developed on CCG Standard Microsoft Office packages to enable an individual to fulfil his responsibilities to the CCG more effectively.

The CCGs Principal Statement of Terms and Conditions of Service state:

"The CCG has the right of ownership to all Intellectual Property including information produced by you in the course of your employment with the CCG. You have an obligation to inform your manager about identified or potential Intellectual Property resulting from your activities and must not sell, assign or otherwise trade Intellectual Property without prior agreement from the CCG.

The CCG wishes to stress that all papers and files, which contain CCG-related information are the property of the CCG and remain so irrespective of origin or authorship."

6.19. Design and use of spreadsheets
Objectives

To ensure the CCG acts only on accurate information which has been produced utilising the minimum of staff resources efficiently and effectively

6.19.1. Best Practise Guidelines

The following Best Practise Guidelines must be adopted by anyone who is either designing or using a spreadsheet.

- **Consistency with Strategy**

  Spreadsheets should only be developed if they are required to meet a business information requirement which cannot be produced by the key financial and management information systems. It is not a cost effective use of resources to spend time and effort producing information from spreadsheets which could be produced from one of the CCGs corporate systems.

- **Specification**

  Spreadsheets should be designed to meet set objectives. Review and monitoring of spreadsheet design should be carried out by authorised persons only. Specification should include controls within the spreadsheet - i.e. protection of all cells other than 'data' cells to be entered by the end user. Where possible, segregation of designer and end user of spreadsheet should be enforced.

- **Approval**

  Spreadsheets should only be implemented and used when, approval of the spreadsheet and controls over it have been authorised by the users line manager or departmental head.

- **Testing**

  Comprehensive and effective testing of all computer programs and systems should be applied, before being used to produce output on which reliance is to be placed - i.e. dummy runs with dummy data.
• **Documentation**

   Technical documentation should be prepared to provide all information necessary for the technical understanding of the model; encompassing

   - the specification document as above
   - design notes, including printouts of macro codes, menus, flowcharts, and range names
   - work files describing the key assumptions used in the model
   - a test log giving evidence of all testing
   - a change log

   The level of user documentation required will depend on who is going to use the model. It may be necessary to issue a full user guide or a brief outline may be all that is required. A description of the purpose and workings of the model is always helpful.

• **Spreadsheet Packages**

   Only the CCG standard spreadsheet package Microsoft Excel must be used.

• **Training**

   End-users must receive sufficient training on the software packages' tools and facilities that are available and how to use them in a controlled way prior to developing any spreadsheets. Ongoing formal technical support will be provided by either an external training company or by CCG Finance or IT Support staff.

• **Security**

   There must be adequate security over spreadsheets to ensure information cannot be copied or changed other than by those personnel authorised to do so. Logs should be maintained and monitored of all access to spreadsheets deemed to be business critical. Passwords used for
key spreadsheets should be changed on a regular basis; the password should be alphanumerical and at least 6 characters in length.

- **Responsibility**

  Personal responsibility should be given to specific individuals for ensuring processed data is accurate and for security of systems from unauthorised access.

- **Commitment**

  All end-users need to share a commitment for striving for consistency in the application of control procedures to their operations. This can be achieved through managers making individuals aware of the importance attached to the whole issue.

**6.19.2. By adherence to the above Guidelines the CCG will have minimised the risks below**

1) Incorrect results may be produced through incorrectly functioning systems.

   - Little or no testing of the operation of packaged software.
   - Inadequate programming standards and documentation of 'in-house' spreadsheet development.
   - Lack of understanding of the system (e.g. No training or technical support).

2) Data may not be available when required or data confidentiality may be breached.

   - Failure to allocate personal responsibility for data accuracy.
   - Possible unauthorised access to data files.
   - Lack of file back-ups.
• No control over down-loading and up-loading of files.

3) Resources may be lost, misused or used inefficiently.

• Inappropriate or incompatible technology may be selected.

• Duplication of processing (i.e. by departments and head office).

• Malfunction of end-users equipment due to connecting of incompatible hardware.

• Lap-tops, modems and disks are valuable and easy to steal - data lost, no back-up.

4) Data processing may be in breach of legal or contractual obligations.

• Data or program corruption via 'viruses'.

• Copying or making extra unauthorised copies of software packages may break licensing agreement regulating their use (Copyright, Design & Patents Act 1998).

6.20. Computer and user access control

<table>
<thead>
<tr>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>To prevent unauthorised computer access</td>
</tr>
<tr>
<td>To restrict access to business and patient information to authorised users</td>
</tr>
</tbody>
</table>

6.20.1. Introduction

Many of the CCGs computer systems are used to store data relating to staff or patient information.

It is therefore vital to restrict access to staff, patients or financial information. Access will be restricted through the implementation of a password system which will only allow those authorised to gain information from the system, and where appropriate amend data, at the level that is necessary for them to function in accordance with their job description. Individual system managers, in conjunction with the IT Operations Manager, will ensure adequate password controls exist and are enforced.
The CCG will institute passwords on all computer systems to identify and authenticate bona fide users.

Security of the system and data contained within implies responsibilities for the individual and their managers.

The CCG will consider as a disciplinary offence any unauthorised attempt to access information, or computer systems which you are not authorised to access. This includes parts of computer systems for which you are not authorised (e.g. personnel records).

Individuals who do not work for the CCG but have a legitimate requirement to access CCG computer systems will have to sign an honorary CCG contract as well as obtaining an agreed level of competence in the use of that section of the system as determined by the System Manager or the CCG Training Department. System Managers must ensure that they the line manager authorising a requirement to access CCG information confirms that a honorary contract has been signed.

We have been asked by NHS Connecting for Health to draw your attention to the attached judgment from the European Court of Human Rights regarding inappropriate access to a patient's medical record.

In the case, a nurse in Finland had been attending a clinic for treatment of HIV. At the same time she was working in a different department of the same hospital. It became apparent that staff in her work department had looked at her medical record and she was denied subsequent employment.

The court ruled that her right to privacy had been breached and she has been awarded compensation.

Whilst a key element of this case was that an individual with a condition regarded as very sensitive lost her job due to breach of privacy, the case underlines the need for the strong access controls and audit trails that are being delivered by NHS CFH.

In the context of the UK Data Protection Act 1998, the judgment provides a clear steer on what is required for health record systems to meet the requirement for there to be a level of technical security appropriate to the nature of the data to be protected. The court was clearly of the view that health care staff who are not involved in the care of a patient must be unable to access that patient's medical record and concluded that "What is required in this connection is practical and effective protection to exclude any possibility of unauthorised access occurring in the first place."
In many cases the NHS has historically relied upon professional codes, deterrent laws and retrospective employment sanctions to safeguard data. It is clear that in future this will be insufficient and that technical access controls that limit access to those who have a legitimate relationship with a patient and audit trails that are able to detect which staff have accessed which records are essential.

6.20.2. Password Allocation

Access to computer systems is restricted to those members of staff that have been issued with an individual identifiable password or series of passwords.

Access to Computer Systems can only be authorised by one of the following:

- The System Owner or their appointed and delegated System Administrator
- Departmental System: Departmental Head/Clinical Director/System Manager
- CCG wide System: Clinical Director/Nurse Manager/Departmental Head/System Manager

A member of staff will be issued with a password to allow them access to their relevant part of any particular computer system only after they have obtained an agreed level of competence in the use of that section of the system as determined by the System Manager or the CCG Training Department.

All members of staff who have not already received training in security and confidentiality issues must be made fully aware of their responsibilities and be booked on to an appropriate training/awareness course at the time their password is issued. The areas to be covered are:

- introduction to and understanding of the basics of the 1998 Data Protection Act
- awareness of the Computer Misuse Act 1990 and its three main sections
- awareness of IM&T policies relating to the use of the system

6.20.2.1. Password Formulation/Changes

Passwords to be a minimum of 6 alpha/numeric characters and they are to be changed at no more than 2 month intervals.
6.20.3. Responsibilities

6.20.3.1. Individuals

The individual member of staff will be responsible for ensuring that his/her password(s) is/are kept secure.

Ideally these should be remembered and written records destroyed, or the user name and passwords be kept separately.

A member of staff will be deemed to have committed a "Breach of Security" if any of the following situations apply:

1. A written record is found of their password which is accessible to any other person other than themselves.

2. They are found to have allowed any other person to access or use the software or data on the system using their password, without authority from the IT Operations Manager.

3. If any other person has been found using their password whether wilfully intended or not.

4. Failure to operate at all times within the CCG policy on confidentiality.

5. Failure to operate at all times within professional guidelines on confidentiality.

Any breach of security as defined above will result in an investigation being carried out by the Line Manager in conjunction with appropriate representation from the IT Support department, at the end of which disciplinary proceedings may be initiated against the individual(s) concerned. In the most severe cases of a "Breach of Security", dismissal of the individual(s) may occur.

6.20.3.2. Managers

In addition to the responsibilities outlined above, the Departmental or Ward Manager also has the following responsibilities:
• **CCG System**

To immediately inform the IT Operations Manager of any changes in a member of their staff's status.

This would include things such as long term sickness, maternity leave and impending termination of contract etc, to ensure system access is rescinded immediately.

To inform the IT Operations Manager of any "Breach of Security", as outlined above, at the earliest possible opportunity. To ensure that all staff within their sphere of authority have received training and are aware of their responsibilities under this policy. To decide in conjunction with the user and IT Operations Manager the operational requirements, in terms of access levels, that each member of staff will need.

• **Departmental System**

To inform the System Administrator as for CCG Systems of changes in staff status.

To inform the IT Operations Manager of any "Breach of Security" as outlined above at the earliest opportunity. To ensure that all staff within their sphere of authority have received training and are aware of their responsibilities under this policy. To decide in conjunction with the System Administrator the operational requirements in terms of access levels that each member of staff will need.

6.20.3.3. **IT Support Department**

In addition to the responsibilities outlined above, the IT support Department will also have the following responsibilities in respect of CCG-wide systems:

- ensure passwords are changed at regular intervals
- maintain a list of all up to date password holders and their access levels
- to maintain an access profile of each user
The above lists to be kept in a secure environment.

- to develop in conjunction with the Internal Auditors the audit trail requirements to ensure that user activity within the system can be monitored and unauthorised attempts at access identified.

In addition, the IT Operations Manager will be responsible for monitoring the effectiveness of this policy and instituting changes as required and agreed with the IM&T Security Officer to ensure system security is maintained.

6.20.3.4. System Managers

It is the responsibility of System Administrators in respect of departmental systems to carry out the following tasks:

- maintain a list of all up to date password holders and their access levels
- ensure passwords are changed at regular intervals
- maintain an access profile of each user
  - The above lists to be kept in a secure environment.
- ensure access to the system is restricted to authorised users only

6.20.4. User Registration

Registration forms are used to authorise the registration of a user to a particular system or systems and can be obtained from the System Administrator or the IT Helpdesk. The level of authorisation is agreed as per section 16.2 and the signature of the two authorisers and the date is entered (see APPENDIX E for an example).

The password(s) is/are issued by the IT Helpdesk.
Smartcards will only be issued in accordance with the CCGs Registration Authority Operational Procedures which involves the production of identification data including at least one photo ID, the printing of the smartcard with the individuals photograph on it and the issuing of role and access rights by their sponsor.

6.20.5. Special Privilege Management

Only allowed to the authorised IT System Administrator and his nominated support colleague.

No-one else within the CCG has or will be given this form of access. Suppliers will be given access in order for them to complete their contractual duties. Passwords will then be changed.

6.20.6. Terminal Log-On Procedures

For the major corporate systems and for all future CCG systems the following criteria for the log-on process will apply:

- display a general notice warning that the computer should only be accessed by authorised users and that access by unauthorised users may constitute an offence under the Computer Misuse Act (1990), for which they may be prosecuted. (see Appendix B)

- not provide, during log-on, help messages that would aid an unauthorised user

- if the current software will permit, then number of unsuccessful log-on attempts allowed will be limited, after which the following actions should take place:
  - the unsuccessful attempt is recorded
  - a time delay is forced before further log-on attempts are allowed
  - data link connections are disconnected

- if the software allows, the maximum time allowed for the log-on process will be limited. If exceeded, the system should terminate the log-on

- if the software allows, then the following information will be displayed on completion of
a successful log-on:

- date and time of the last successful log-on
- details of any unsuccessful attempts since the last successful log-on

- Smartcard logon is by use of the card being inserted into a card reader or card reader slot on a keyboard and the entry of the PIN number known only to that card holding individual

6.20.7. User Identifiers

Each user will be issued with a unique identifier (user-id) for their personal and sole use. The user-id will give no indication of the user's privilege level.

Smartcards combine the information on the card with the roles and authorities for those roles and the individual held on the security area of the “NHS spine” plus the individual's PIN.

6.20.8. Inactive Terminals

In high risk areas systems that access sensitive data are set to time out after a pre-set time interval.

This will be assessed and agreed with the Manager of the user's department and the IT Operations Manager.

On timeout, either:

- Application will require correct password be entered
- Application will drop link and require re-log in

Users are responsible for logging off terminals or PCs when leaving them unattended. PCs or terminals should be secured by a password access control when not in use.
6.20.9. Smartcard Usage

Staff who require access to national IT systems to carry out their duties will on production of suitable identification documentation be granted a Smartcard with appropriate permissions to carry out their duties. They will then be asked to enter a PIN number which they must keep secret and not allow anyone else to use their card to access patient information. Further information on the use of Smartcards and the CCG Registration Authority rules can be found in the CCGs Registration Authority Operational Procedures.

6.21. Application access control

<table>
<thead>
<tr>
<th><strong>Objective</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>To prevent unauthorised access to information held in computer systems</td>
</tr>
</tbody>
</table>

This level of access is ONLY permitted to the professional IT staff under the management control of:

- IT Operations Manager
- Departmental System Manager
- Application Support Manager

6.21.1. Changing or By-passing Access Rights

- Within the CCG ONLY IT Support staff have full access rights
- No-one will be allowed to by pass their access rights, anyone found to be doing so will be subject to disciplinary action

6.21.2. Emergency Access Rights for Suppliers Technical Support Staff or Maintenance Engineers
• will be given either "root" or "supervisor" ID & password

• will be changed on completion of work

6.21.3. System Utilities Access Restriction

The use of system utilities is restricted to the professional IT Support staff and controlled by the IT Operations Manager who ensures:

• password protection for system utilities

• limitation of the use of system utilities to the minimum number of CCGed, authorised users

6.21.4. Control of Access to Program Source Libraries

• In most cases Source libraries are under the control of the system suppliers, however where the IT Support Department Staff have developed systems in house they will ensure access to source libraries is strictly controlled

• Vendor supplied software packages must be used without modification by CCG staff.

If any changes are necessary, these should be obtained from the vendor.

6.22. Monitoring system access and use

<table>
<thead>
<tr>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>To detect unauthorised activities</td>
</tr>
</tbody>
</table>

6.22.1. Monitoring System Use

6.22.1.1. Security Unusual Incident Log

This will be kept by the IT Operations Manager and will be referenced by a unique identifier to the documentation retained on each incident on completion of his investigations (Ref. Section 7).
6.22.1.2. Other areas that will be monitored will be:

Tracking of selected transactions will be done on a "reason for concern" basis.

6.22.2. System Audits

These will be carried out on a spot check basis as and when resources are available and will:

- update the IT Equipment/Software Register (Ref. 3.1.4) and identify ownership
- record the location, brief description and where possible the serial number of the equipment
- identify and produce an audit trail of the software and files held on the computer being audited
- any breaches of rules encompassed within this document and/or current legislation will be reported to the IM&T Security Officer.

6.22.3. Clock Synchronisation

- The CCG Domain Controller server in the computer room takes its time from an atomic clock and is the master clock source within the CCG for all servers
- PCs run regularly synchronises the PCs clock to the CCG Domain Controller server clock.

6.23. Patient information

<table>
<thead>
<tr>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>To restrict access to identifiable patient information to those authorised to see it in line with the principles outlined in Caldicott Report</td>
</tr>
</tbody>
</table>

Principle 1 - Justify the purpose(s)
Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

**Principle 2 - Don’t use patient-identifiable information unless it is absolutely necessary**

Patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

**Principle 3 - Use the minimum necessary patient-identifiable information**

Where use of patient-identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

**Principle 4 - Access to patient-identifiable information should be on a strict need-to-know basis**

Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

**Principle 5 - Everyone with access to patient-identifiable information should be aware of their responsibilities**

Action should be taken to ensure that those handling patient-identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

**Principle 6 - Understand and comply with the law**

Every use of patient-identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.
6.23.1. Identifiable Patient Information

Wherever possible anonymised data will be used by issuing information in:

a) summary form

b) by use of the CCG identification number

or

c) by use of the NHS Number (when this is available and practical)

Data sent to other NHS bodies and other authorised organisations will be sent in the most secure format available, and identifying information will be sent on separate disks/tapes in separate envelopes from the related clinical data. The sets of data will be capable of reassembly by means of a unique identifier present on both files. **Identifiable data will only be sent within the terms of the Caldicott Principles.**

Data sent via the Walsall NHS Network is protected by the security regulations pertaining to this network and is regarded as secure, however data sent via the N3 network is not deemed as Secure and should be encrypted.

6.23.2. Access Limitations

These will be controlled as described in the previous sections of this document.

The standard applied will be the "need to know".

The limitations will be the restrictions in separation of data access within the computer systems in use.

Only authorised persons or groups identified within the CCGs declaration to the Data Protection Registrar will be permitted access to information in any particular system.
6.23.3. Medical Oversight

Arrangements and policy for access to person-identifiable data will be overseen by the Caldicott Guardian or deputy.

The IM&T Security Officer will have direct access to the designated CCG and/ or Caldicott Guardian for guidance on policy.

6.23.4. Holding of Patient Information outside the CCG

Staff without a clinical reason must never transfer patient identifiable information from any CCG computer equipment to any computer equipment not owned by the CCG e.g. their own computer or Personal Digital Assistant (PDA).

**Staff carrying out work for the CCG** that requires holding personal patient or employee data on a pc, laptop or personal digital assistant (PDA) not owned by the CCG, are covered by the CCG registration on condition they comply with confidentiality and security guidelines set out in the CCG Information Management & Technology Policies.

**Staff holding personal patient or employee data for personal use**, e.g. student case histories, research data and doctors’ project work, on a pc, laptop or personal digital assistant (PDA) not owned by the CCG, will need to register with the Information Commissioner’s Office under the Data Protection Act 1998. This is a requirement by law and failure to notify is a criminal offence.

Information relating to a living individual who can be identified by the information, or information that does not in itself identify an individual but when combined with other information you hold could be used to identify an individual, is classed as personal data. Examples may include clinical audit data, student case histories, research data and doctors’ project work.

If you do hold personal data on your own pc, laptop or personal digital assistant (PDA) for personal use, you have a legal obligation to comply with the eight principles of good information handling (Data Protection principles) and to notify and register with the Information Commissioner as a Data Controller. If confidentiality is breached you could be prosecuted under the Data Protection Act. You will not be covered by the CCGs registration. If in doubt you should register under the Act.
Registration is a simple process and can be completed online at www.informationcommissioner.gov.uk or a form can be obtained from:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

6.24. Data validation

<table>
<thead>
<tr>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>To prevent less, modification or misuse of data</td>
</tr>
</tbody>
</table>

6.24.1. Input Data Validation

6.24.1.1. Referential integrity and validity checking

- Will be implemented where possible and practical.
- The degree to which such facilities are available in systems under consideration for procurement will be taken into account in the selection process.

6.24.1.2. Reconciliation across Modules and Systems

Were recommended/advised by the audit department of the CCG and were practical such reconciliation procedures will be put in place by the Systems Manager in conjunction with the IT Operations Manager.

6.24.1.3. Loss or Corruption of Data

Must be reported to the IT Operations Manager who will inform the relevant system manager

Stating where known:-

- date and time of discovery
6.24.2. Internal processing validation.

6.24.2.1. Validation Checks

Depending on the nature of the system concerned one or more of the following may be carried out.

- session or batch controls, to reconcile data file balances after transaction updates.
- balancing controls, to check opening balances against previous closing balances.
- validation of system generated data.
- hash totals of records and files.

6.24.2.2. Audit Trails

Will where possible; be kept for each system to allow tracing of all system transactions including failed transactions. The retention period of the audit trail will be as agreed with internal audit or in accordance with HSC (99)053 - For the Record: Managing NHS Records.

6.25. Data encryption

<table>
<thead>
<tr>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>To prevent un-authorised access of patient information</td>
</tr>
</tbody>
</table>

6.25.1. CCG Encryption

6.25.1.1. The CCG has completed a program of encrypting all laptops using the nationally procured product Safeboot. There may be some older laptops which will not run if encrypted and these will be looked at with a view to replacement.

It is the responsibility of the user to ensure the laptop they use has the Safeboot Software installed. A call can be logged with the ITHelpdesk to have the Software installed.
With regard to USB connected devices:

- CCG policy states that the use of non encrypted IT Support procured memory sticks are strictly banned. IT will maintain a list of approved memory sticks.

- PDAs which can be encrypted will be allowed to connect via USB. However the CCG cannot be held liable for any personal device which is plugged into CCG equipment and if you choose to connect your device you do so entirely at your own risk. The CCG must warn that if the Safeboot software starts to encrypt any device connected to any CCG piece of computer hardware it may render them un-usable.

- Mobile phones are likely to work if connected via USB to synchronise with Microsoft Outlook, however attempts to use any memory card in the phone will result in the card being encrypted and un-useable. So if you choose to connect your device you do so entirely at your own risk.

6.25.2. Email encryption

The CCG will be encrypting emails where any confidential and or patient identifiable information is sent. All attachments are planned to be encrypted. Circumventing this software will be deemed a disciplinary offence.

6.26. Security of application systems

**Objective**

To ensure that IM&T projects and support activity are conducted in a secure manner


6.26.1.1. It will be the responsibility of the commercial supplier under the terms and conditions of his contract to ensure that all new software releases are quality assured before live use on any of the CCGs systems.

6.26.1.2. The procurement process will define within the contract schedules the criteria for measuring the acceptability of the software. The designated Departmental Manager will be responsible for ensuring that the criteria, has been met before the product is accepted.
6.26.1.3. For small systems development, the CCGs Small IT System Development Policy (Section 14) will be followed.

- In the case of commercially provided systems, be they either off the shelf, bespoke or a mixture of the two, it will be the responsibility of the commercial supplier to ensure testing and quality assurance. It will be the responsibility of the IT Operations Manager to assess the product and reliability of the supplier prior to procurement.

- In the case of small development in house it will be the responsibility of the designated Departmental Manager to ensure that they are tested to a level where he is prepared to accept responsibility for their release.

  + They will be fully documented.
  + They will be version controlled and dated.
  + Secure copies of the software and related documentation will be retained within the department.

6.26.2. Protection of System Data

6.26.2.1. The access control procedures which apply to operational application systems and to test application programs.

6.26.2.2. Except where standards and procedures have been agreed (for example the copying of CMDS data for purchasers), the copying, archiving or dumping of any data should be authorised by the IT Operations Manager.

6.26.2.3. Live sensitive data should not be used for testing, training or demonstration purposes unless it is transformed such that identification of the original contents is not possible, or the permission of the person whose data it is has given permission, or if the sole audience of staff who in the course of their duties normally have access to this data.

6.26.2.4. Live and test data files must always be logically separated.

6.27. Business continuity planning

<table>
<thead>
<tr>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>To be able to maintain essential business activities after any unforeseen major failure or disaster</td>
</tr>
</tbody>
</table>
The CCGs approach is to assess the risks and take action to minimise or eliminate the risk.

6.27.1. Primary Computer Room

The room was purpose built as a computer facility, of solid construction.

- Access is restricted to authorised personnel only
- Area is protected by automatic fire detection systems
- Area is protected by a security system and electronic and manual security locks
- Power to computer and communications equipment is supplied via UPS
- Computer room has feed from main hospital generator, which feeds the UPS, air conditioning and lighting in the event of power grid failure.
- Computer room protected by air sampling fire detection system
- No water supply run through the area
- Combustible material is kept to a minimum in the computer room

6.27.2. Business Continuity Planning

A Business Continuity Planning Manual covering the following area is held by The IT Operations Manager and relevant system managers on critical CCG Corporate systems.

The document covers the following areas:

- a formal, documented, assessment of how long users could manage without each computer system.
• a formal, documented, assessment of the criticality of each system, including the impact of the short, medium and long term loss of the system on business activities.

• identification and agreement of all responsibilities and emergency arrangements.

• documentation of agreed procedures and processes.

• a formal assessment of how resilience and continuity will be achieved.

Resilience measures may include duplicating parts of the installation to reduce the risk of breakdown stopping its operation. Continuity measures may include falling back to a manual system or identifying alternative installations or sites to which the system can be moved if the computer is lost. The first step is meeting the users’ requirements for continued operation is to identify the measures needed.

6.27.3. Proposed on Completion of the Planning Process

• copies of plans will be held both on-site and in a secure location off site.

• managers of the systems and departments concerned will be issued with copies to keep both at work and at home.

• a register of managers issued with particular plans will be kept by the IM&T Security Officer.

• copies will be version numbered and dated.

• IM&T Security Officer will hold master copies of all plans and will be responsible for issuing plans and updates.

• a single framework plan will be maintained to obtain consistency.

6.27.4. Testing and Updating Business Contingency Plans (Proposal)

• Test schedule will be drawn up for each plan.
• Plans will be reviewed and updated as necessary at agreed intervals.
Changes to plans will be formally authorised by the Information Steering Group and these will then be implemented and version controlled.

6.28. Compliance

<table>
<thead>
<tr>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>To comply with any statutory obligations</td>
</tr>
</tbody>
</table>

6.28.1. Control of proprietary software copying.

ONLY Licensed software registered with the IT Support Department is permitted.

It is a criminal offence to install and use unlicensed software, in the UK, under the Copyright, Designs and Patients Act (1988).

Audits of software will be carried out at a predetermined frequency in conjunction with Internal Audit and subject to availability of resources.

6.28.2. Safeguarding of Organisation Records


6.28.3. Data Protection

Nominated Officer for the CCG is

Head of Health Records

- Systems Managers are responsible for ensuring that their systems are registered with the Data Protection Registrar
• Help and assistance will be given by the Head of Performance & Information

• Data Protection Act (1998) see APPENDIX A

• The Protection and Use of Patient Information (refer to CCGs policy & HSG (96) 18)

6.28.4. Prevention of Misuse of IM&T Facilities

6.28.4.1. Employees of an NHS organisation and any third party users must be informed that no access to systems is permitted except where this has been formally authorised and documented.

6.28.4.2. Any use of IM&T facilities for non-business or unauthorised purposes, without management approval will be regarded as improper use of the facilities.

6.28.4.3. The Computer Misuse Act (1990) see APPENDIX B introduced three criminal offences:

• unauthorised access

• unauthorised access with intent to commit a further, serious offence

• unauthorised modification of computer material.

6.29. Risk assessment

<table>
<thead>
<tr>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>To ensure compliance of systems with the current Information Governance Toolkit</td>
</tr>
</tbody>
</table>

Compliance with the current Information Governance Toolkit and subsequent assessment of risks will be undertaken for all new IT systems and major updates.

Mitigation and management of any identified risks will be the responsibility of the project board for new system the system owner system administrator and the IT Operations Manager.

Four main functions of Risk Assessment will be considered for each critical system.
a) **identification of assets** - assets within the risk assessment to be identified, valued and documented.

b) **evaluation of impact** of identified risk refer to Appendix D matrix.

c) **assessment of the likelihood** of the risk occurring.

d) **identification of appropriate countermeasures** to mitigate the risks.

### 6.30. System planning, procurement and acceptance

**Objective**
To ensure that the procurement of IM & T systems is conducted fairly, legally, according to the relevant NHS guidelines and standards, and yields value for money to the public purse.

### 6.30.1. Project Organisation, Planning and Control

The implementation of IM&T systems will be managed using the pragmatic application of the PRINCE project management methodology. Procurement is a distinct stage of such a project and covers all activities from project initiation through to contract signature.

Procurements will be initiated under the approval of the Information Executive Group and will be directed by a Project Board, which will include senior representation of business, user and technical interests. A Project Manager will be appointed by Informatics or a senior member of the main user department. The project manager will provide a Project Co-ordinator to structure, facilitate and document the process.

A Project Team will be appointed to undertake the detailed work of requirements specification and system/service evaluation. This Team will comprise representatives from the main user departments working along side technical staff.

A formal project plan will be drawn up for approval by the Project Board. This will specify the objectives, scope, deliverables, activities and timescale of the procurement.
Progress against the plan will be monitored by regular meetings of the Project Board who will receive regular highlight reports prepared by the Project Co-ordinator. These will be copied to the Information Executive Group.

6.30.2. Outline and Full Business Cases

Every procurement must be supported by an approved business case. In general, approval of the business case is a two stage process. The first task is production of an outline business case for approval before the procurement itself begins in earnest. A full business case will be produced once the full costs and cost/benefits of the procurement are confirmed.

The full extent of the business case and business case approval process are dependent primarily upon the value of the procurement. Rules and requirements for significant IM&T investments are specified in the NHS Capital Investment Manual and the CCGs local Capital Planning regulations.

However, all business cases will include:

- The relevance of the procurement to the CCGs Business Plan and IM&T Strategy.
- The business objectives of the system.
- The costs of the options identified together with economic and financial analyses.
- An investment appraisal of the options for achieving these objectives.
- The benefits of the preferred option and a benefits realisation plan.
- An assessment of the risks involved and their proposed management.

6.30.3. Procurement Process

The procurement itself will be conducted according to European Union and GATT (General Agreement on Trades and Tariffs) regulations for the procurement of goods and services within the public sector. The resulting contract will be drawn up and signed according to English law.

The nature and process of the procurement will also be structured according the current NHS guidelines. It will also comply with the CCGs Standing Financial Instructions.

A nominated representative from the procurement department will be invited onto the project board.
The main steps in the procurement of a significant system, apart from progress of the business case, will be:

- Check suppliers listed in OCG Catalist contract
- Market research for effective solutions.
- Preparation of an OBS (Output Based Specification) for issue to prospective suppliers.
- Advertisement of the procurement in the OJEC.
- Sifting of responses for potential suppliers.
- Short listing of potential suppliers through interviews, analysis of proposals, demonstrations and site visits.
- Development of draft contracts and proposed implementation plans with short listed suppliers.
- Competitive tender normally involving at least two suppliers.
- Evaluation of tenders and recommendation of a supplier against pre-determined criteria.
- Award of contract.

6.30.4. System Acceptance

The contract negotiated will include specific sections detailing the respective responsibilities of the Contractor and the CCG. The responsibilities of the CCG, in particular the commitment of resources to meet an agreed implementation timetable must be thoroughly understood and accepted by the Project Board and user departments before contract signature.

Part of the implementation activity will relate to system acceptance testing. A specific section of the contract will describe the testing criteria which will be used to establish provisional and final acceptance. Acceptance testing will in part be technical and will in part relate to the documented system functionality and delivery of expected benefits. System acceptance will represent a key trigger point for release of funds within the contract payment profile.

6.30.5. Benefits Realisation

The business case will include a benefits realisation schedule. Implementation activity should be geared towards realisation of benefits within the documented timescale. It is likely that the full benefits of a major system will not be realised until some time after the implementation is complete. Nevertheless, the project will not be closed down, until a benefits realisation review has been conducted, a project closure report produced and any resulting actions have been taken.
6.31. Mobile working-Remote Working policy and procedure

6.31.1. Objectives

To manage and prevent unacceptable risks arising to the organisation and other NHS information assets through the use of unapproved or unsafe home working facilities.

The CCG recognises that by providing staff with remote access to information systems, risks are introduced that may result in serious business impact, for example:

- unavailability of network, systems or target information
- degraded performance of remote connections
- loss or corruption of sensitive data
- breach of confidentiality
- loss of or damage to equipment
- breach of legislation or non-compliance with regulatory or ethical standards.

6.31.2. Remote working procedures

This section outlines the control procedures in place for remote working.

- Remote working must be approved by the Head of Service only on receipt of signed approval form (see Appendix Q) will the individual be granted remote access.
- Connection will only be made to the CCG network secure broadband access.
- A single entry point will control access to the network, e.g. firewall and secure ID Token.
- Users must authenticate to the network, by using two-factor authentication
  - Secure Token across a broadband line
  - Relevant CCG network user account (User name)

6.31.3. Terms and Conditions

- Employees must identify themselves to the network by using their own logon credentials.
- Two-factor credentials must be kept confidential at all times.
- Lost tokens must be reported immediately so accounts can be disabled, this would also need to be documented as a security incident.
- Employees who are leaving the company must ensure that all equipment is returned to IT Logistics so accounts can be disabled on the last day of employment.
• If an employee’s contract is terminated, it is the responsibility of HR to inform IT Services to ensure the necessary accounts are disabled.

• Any agreement on remote working is not permanent and may be brought to an end at any time by the member of staff or the CCG. An authorisation will be based on the needs of the CCG, the job, and the department.

6.31.4. Provision of Equipment

The CCG will not provide or maintain a home PC or broadband connection, but will provide the necessary additional equipment to enable remote connection to the CCG’s network if necessary and required. This equipment could include:

• An active Token, synchronised to the network to provide once only passwords for secure login;

The CCG will set-up and test the CCG supplied equipment for home use to ensure that CCG software is correctly installed and the connection to the CCG’s network is functioning and secure. Supplies necessary to work at a remote site should be obtained during a work period in the conventional workplace.

Laptops will be provided on an exceptional basis and at the discretion of the relevant director/head of function or service. Laptops are not primarily for home working but for staff who need to regularly move from one workplace to another in the course of their normal work.

The CCG is not liable or responsible for the support of home equipment (such as broadband connection) except in respect of the equipment and software detailed above and directly relevant to remote access the CCG’s systems.

The CCG monitors who logs into the network and can monitor which Internet and NHSnet sites are visited by any one user. Access to the remote access server is provided on the understanding that this is the case.

Any hardware or software provided by the CCG remains the property of the CCG and shall be returned at the end of the remote working arrangement. An equipment/software inventory will be completed by IT Logistics for assigned CCG equipment to be used off-site.
Products, documents and other records used and/or developed while working remotely remain the property of and will be available to the CCG. This information is subject to CCG policies regarding confidentiality and access, including the Caldicott recommendations.

CCG owned software may not be duplicated. Staff working remotely using CCG software must adhere to the manufacturer’s licensing agreements.

Each member of staff working remotely is responsible for protecting the integrity of copyrighted software, and following policies, procedures, and practices related to them to the same extent applicable in the conventional workplace. The member of staff must take all precautions necessary to avoid contamination of data for example by use of unauthorised software that may contain a computer virus.

The member of staff working remotely is responsible for setting up and maintaining an adequate workspace at the remote workplace and for ensuring that it is maintained to the same standards as apply to the conventional workplace.

Purchasing and maintenance of personal office furniture or equipment eg desks, filing cabinets, answering devices, etc, is the responsibility of the member of staff working remotely.

### 6.31.5. Health and Safety

Most of the regulations under the Health and Safety at Work Act 1974 and all other current health and safety legislation, apply to staff working remotely as well as when working in their conventional workplace.

Authorisation for remote working is subject to satisfactory completion of Appendix Q.

The CCG will have the same responsibility for job-related accidents or injuries to the member of staff at the remote workplace that it has at the member of staff’s conventional workplace.

The CCG is not responsible for any injury to any other person at the member of staff's remote workplace.

The member of staff is responsible for establishing and maintaining a designated, adequate workspace at the remote workplace. This space should be maintained to the same safety and other standards as are applicable in the conventional workplace. With reasonable notice and at mutually agreed times during working hours,
the CCG may make visits to the home or remote location to assess health safety and welfare of the member of staff.

The member of staff is responsible for telephoning in to the conventional workplace at scheduled times agreed by prior arrangement with their line manager. This is a health and safety measure considered standard practice within remote working arrangements.

6.31.6. Health & Safety Responsibilities

The CCG cannot accept the responsibility for the health and safety of a remote working environment

- If the remote site is, another CCG or facility providing a service to the user the Health and Safety of the user will fall under the remote site’s health and Safety guidelines.
- If the remote users is working from home it will be the individual’s responsibility to ensure that they conduct any work for the CCG in a safe and practical manor as they would if situated in an office environment within their conventional workplace.

6.31.7. Reimbursement

The CCG will not reimburse staff for the use of any privately owned equipment, nor will it pay for the broadband connection.

6.31.8. Confidentiality

As the NHSnet is a closed network and access from other networks is very strictly controlled, staff should be aware that the greatest risk to security is posed by those within the network, and not by outsiders. The NHSnet cannot protect systems from the actions, legitimate or otherwise, of other users. Therefore, all staff should be especially aware of the CCG’s security and Internet and E-mail policies. Staff should also ensure that they are meeting the requirements of the Data Protection Acts 1984 and 1998, and at all times behave in accordance with UK law.

Staff working on CCG or associated organisations material/work must at all times take extreme care to ensure that confidentiality is maintained. Sensitive and confidential material must not be taken out of the conventional workplace without prior approval by a member of staff’s line manager.
6.32. System Security Policy

6.32.1. Introduction
Information and information systems are important corporate assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support the operation and continued success of the CCG.

The aim of the CCG's System Security Policy is to maintain the confidentiality, integrity and availability of information stored, processed and communicated by and within the CCG.

A mandatory requirement for British Standard certification is to have a clear understanding of the information assets involved and to document these in an Information Asset Register.

The Information Asset Register will provide details of the classification and ownership of each of the information assets, and also forms a key input to the Risk Assessment, another mandatory requirement for certification.

The purpose of this Information Asset Register is to identify the different types of information processed, stored and communicated by the CCG.

It is important to ensure that the Information Asset Register is kept under control and updated as necessary. The Information Asset Register should be updated every time the details of one of the information assets change including the Information Asset Owner (IAO).

An information Security System can exist in several formats, both in terms of the physical media on which the data is stored and in terms of whether it is permanently or temporarily stored. This affects the security controls that may be applied as a result of the Risk Assessment, e.g. paper documents may be locked in a cabinet whilst files stored on a network drive may require setting of system access rights for protection.

The sub sections below detail each of these basic categories.

**Paper**
Much of the information exists in conventional paper form, although it is likely that originally it would have been produced on a computer. Also in this category are printouts of electronic documents, files and logs.

**Electronic**
This is data that is stored electronically, either within server or client equipment or on electronic media. Data stored within the equipment is most commonly stored on an internal
hard disk or on central storage such as Storage Area Networks (SAN’s). Protection of this is ensured through the physical access to the machine and through the logical controls that are managed through the configuration of the operating system.

This data may be backed up or copied onto other media, including floppy disks, CD-ROMs/DVD’s, tapes, USB devices and Pen Drives. These are protected through physical measures in a similar manner to paper documents. A summary of the media types is given below:

**Floppy Disk**
These are 3.5 inch diskettes with a storage capacity of 1.44Mb readable by virtually any computer.

**CD-ROM**
These have a capacity of 650Mb and exist in two formats, CDR, which can be written to once and cannot be erased and CDRW, which can be rewritten in a similar manner to floppy disks;

**DVD-ROM**
These have a capacity of 4.7 Gb and exist in two formats DVDR which can be written to once and cannot be erased and DVDRW, which can be rewritten.

**Pen Drives/USB Drives/Memory Sticks**
This are portable storage devices which can be rewritten as often as the user likes the size of the storage is up to 16Gb and over depending on current technology.

**Tape Storage**
Tape cartridges that require a specialist device to read and write data to. These can have various capacities, up to many tens of Gbs.
Systems shall incorporate the following security countermeasures:

- Physical security measures (E.g. secure room, cabinet, etc), Logical measures for access control and privilege management
  - For more information see the CCG Physical and Environmental Security Standards document

- Network security measures (E.g. firewalls, network segregation, etc)
  - For more information see the relevant systems Operations and Services Handbook.

6.32.2. Server Room Environmental Security

- The CCG receives facilities management services that operate through a Service Level Agreement with the Skanska Facilities Management (SFS).

- The Key IT equipment Communications rooms have access controlled for further information see the CCG Physical and Environmental Security Standards document.

6.32.3. Physical Security

All personnel needing to have access CCGs IT Communications rooms will comply with the CCG Physical and Environmental Security Standards document.

6.32.4. Systems Security

Systems shall incorporate the following security countermeasures:

- Physical security measures (E.g. secure room, cabinet, etc), Logical measures for access control and privilege management
  - For more information see the CCG Physical and Environmental Security Standards document

- Network security measures (E.g. firewalls, network segregation, etc)
  - For more information see the relevant systems Operations and Services Handbook.
7. IMPACT ASSESSMENT

7.1. Risk Implications / Risk Assessment

The major risks to managing this CCG’s Internet, email and phone usage have been assessed and when followed this policy should mitigate or eliminate those risks. To minimise any future risk there will be an on going development and review programme.

8. LINKS TO OTHER CCG POLICIES

- Mobile Phone Policy
- Fraud Corruption Policy
- Disciplinary Policy
- Whistle Blowing Policy
- Mobile Telephones Policy
- Safe Haven Policy

9. LINKS TO EXTERNAL STANDARDS

- Criminal Justice and Immigration Act 2008
- CFH Statement of Compliance information
  http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igsoc
- Data Protection Act 1998
- Human Rights Act 1998
  http://www.opsi.gov.uk/ACTS/acts1998/ukpga_19980042_en_1
- Computer Misuse Act
- Regulation of Investigatory Powers Act
  http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1
- Copyright, Designs and Patents Act 1988
- Trade Mark Act 1994
- Interception Of Communications Act 1985
- Common Law Duty of Confidentiality
- Fraud Act 2006
10. MONITORING, CONTROL AND AUDIT

10.1. Monitoring

All staff should be made aware and understand that IT Services and HR are responsible for establishing Policy Enforcement and monitoring, of any access to the CCG network to establish breaches of acceptable use and security and that staff accept that all, or any of their resource usage may be monitored.

Sites that are not work related that are found to be excessively used and have a detrimental effect to network performance will be blocked.

The CCG has in place routines to regularly audit compliance with this and other standards. In addition it reserves the right to monitor usage and content where it suspects that there has been a breach of policy.

If there is evidence that you are not adhering to the guidelines set out in this policy, the Organisation reserves the right to take disciplinary action, which may lead to a termination of contract and/or legal action.

The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees’ electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

In addition communications may be monitored (but not recorded) for the purpose of checking whether those communications are relevant to the purpose of the CCG’s business, and the employees position with the CCG. Any monitoring will be undertaken in accordance with the above act and the Human Rights Act.

This encompasses all applications, network access and includes Internet access e-mail and where appropriate phone usage. IT Services are responsible for ensuring that comprehensive audit tools are in use which enforce policy and monitor network usage for breaches of
the security policy and log all users by name, and record the Internet sites visited or accessed by IP address and URL, the time of day the sites were accessed and for how long, and if a file transfer took place.

10.2. Reporting
Standard reporting automatically identifies the top users of the Internet each month, these along with reports of sites categorised as inappropriate are also examined and type of usage evaluated, offenders of the rules/guidelines laid down in this policy may be reported to their Line Manager and appropriate action as deemed necessary taken.

Email and phone logs are also reviewed for breaches of this policies rules and guidelines.

10.3. Validity of this Policy
This policy will be reviewed under the authority of the Director of Informatics.

11. BEST PRACTICE, EVIDENCE AND REFERENCES

N/A

12. APPENDICES

12.1. Appendix A - The data protection act 1998

1. THE DATA PROTECTION ACT 1998

An Act to make provision for the regulation of the processing of information relating to individuals including the obtaining, holding, use or disclosure of such information.

1.1 NEW ELEMENTS
- Principles apply to all controllers
- Manual records (e.g. Health records / Personnel records etc)
- Legitimacy of processing conditions
- Sensitive data rules (e.g. health, sexuality etc)
- Freedom of expression
- Automated decisions
- Transfer to non-EU countries (e.g. where info is transcribed)
- Individual rights

1.2 BASIC DEFINITIONS OF 1998 ACT

Data is information which

- is being processed by means of equipment operating automatically in response to instructions given for that purpose, or
- is recorded with the intention that it should be so processed, or
- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or
- does not fall within the above but forms part of an accessible record e.g., Personnel / Medical records

Personal data means data which relate to a living individual who can be identified

- from those data, or
- from those data and other information in the possession of or likely to come into the possession of the data controller,
- and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive personal data means personal data as to the data subjects
- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- membership of a trade union
- physical or mental health or condition
- sexual life
- criminal offences
- criminal proceedings and convictions

Processing means

- obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including
- organisation, adaptation or alteration, or
- retrieval, consultation or use, or
- disclosure by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction.

Relevant filing system means

- any set of information relating to individuals to the extent that, although the information is not automatically processed, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Accessible record means

- A health record (information relating to physical or mental health made by or on behalf of a health professional in connection with the care of the individual), or
- An education record (records relating to pupils at a school processed by the governing body or a teacher), or
- An accessible public record (housing and social services records).

**Data Controller / Data Subject means**

- Data Controller is a person who (alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed.
- Data Subject means an individual who is the subject of personal data.

**Data Processor / Third Party means**

- Data Processor means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
- Third Party means any person other than the data subject, the data controller, any data processor or other person authorised to process data for the data controller or processor.

**Recipient means**

- any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing
- but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry made in the exercise of any power conferred by law.

**The Special Purposes means**

- any one or more of the purposes of journalism, artistic purposes, literary purposes.
2. PRINCIPLES

2.1 FIRST PRINCIPLE

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless -

  a) at least one of the conditions in Schedule 2 is met, and

  b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2.2 SECOND PRINCIPLE

- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

2.3 THIRD PRINCIPLE

- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

2.4 FOURTH PRINCIPLE

- Personal data shall be accurate and, where necessary, kept up to date.

2.5 FIFTH PRINCIPLE

- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

2.6 SIXTH PRINCIPLE
• Personal data shall be processed in accordance with the rights of data subjects under this Act.

2.7 SEVENTH PRINCIPLE

• Appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

2.8 EIGHTH PRINCIPLE

• Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3. SCHEDULE OF CONDITIONS
3.1 SCHEDULE 2 CONDITIONS

- consent of the data subject
- necessary for performance of a contract with the data subject
- legal obligation
- to protect vital interest of the data subject
- to carry out public functions
- to pursue legitimate interest of the controller unless prejudicial to interest of the data subject.

3.2 SCHEDULE 3 CONDITIONS

- explicit consent of the data subject
- to comply with employers legal duty
- to protect vital interests of data subject or another person
- carried out by certain non-profit bodies
- the information has been made public by the data subject
- in legal proceedings
- exercising legal rights
- to carry out public functions
- for medical purposes
- for equal opportunities monitoring
- as specified by order
12.2. Appendix B - Computer misuse act 1990

COMPUTER MISUSE ACT 1990

This document summarises the Computer Misuse Act 1990, Chapter 18, a full copy of which can be obtained from the IT Operations Manager if required.

The computer Misuse Act which became law on 29 August 1990 makes it a criminal offence for anyone to access or modify computer programs or data or to attempt to do so, without the authority of the owner. The Act provides a framework for police prosecution of people who misuse computer. Enforcement of the Act is the responsibility of the police. CCG have introduced computer access controls to clearly identify those who are authorised to use computers and to what level, to facilitate enforcement of the Act against offenders.

The Act deals with three specific offences - unauthorised access to computer programs or data, unauthorised access with a criminal content and authorised modification of computer programs or data which is being held in the computer.

Unauthorised Access

This offence is designed not only to deal with hacking but also users who access parts of the computer system that they are not authorised to access for example, a person may be authorised to access Care Plans but not personnel data. If personnel data is accessed then an offence has been committed.

Section 1 (1) of the Act reads:

A person is guilty of an offence if:

a) He causes any computer to perform any function with intent to secure access to any program or data held in a computer.

b) The access he intends to secure is unauthorised, and
c) He knows at the time that he causes the function that that is the case.

To prove an offence has been committed it is necessary to show:

- That the access was deliberate.
- That the access was unauthorised.
- That the person carrying out the offence knew that it was unauthorised.

Many possible excuses are removed by section 1(2) which states that:

The intent a person has to have to commit an offence under this section need not be directed at:

a) Any particular program or data.

b) A program or data of any particular kind or

c) A program or data held in any particular computer.

A person found guilty of an offence under Section 1 would be liable to a fine of up to £2,000 or imprisonment for up to six months or both.

**Ulterior Intent**

Unauthorised access for the purpose of committing a serious crime is viewed more gravely.

**Section 2 (1) of the Act states:**
A person is guilty of an offence under this section if he commits the "unauthorised access offence" with intent:

a) To commit an offence, or
b) To facilitate the commission of an offence (whether by himself or by some other person).

To prove the ulterior intent offence it must be shown that the accused:

- Deliberately accessed the computer.
- Did not have authority to do so.
- Knew that he was not authorised to access the computer.

A person found guilty of an offence under Section 2 of the Act is liable to a maximum sentence of five years imprisonment and/or an unlimited fine.

**Unauthorised modification**

The unauthorised modification offence means causing any modification of programs or data held in the computer knowingly that this is unauthorised and with the deliberate intent to impair the operation of the computer.

The introduction of viruses, Trojan horses, logic and time tombs are covered by this section.

It is immaterial under the Act if the modification is permanent or temporary. The only point of importance is that there is, an intent to impair the computer system and it does not matter if the damage is caused immediately or in the future.

This offence is covered by Section 3 of the Act. It states that:

A person is guilty of an offence if:
a) He does any act which causes an unauthorised modification of the contents of any computer, and

b) At the time when he does the act he has the requisite intent and the requisite knowledge.

To be proved guilty the modifier must have the "knowledge" that he is unauthorised to carry out the change and the "requisite intent" must be malicious. This is further defined in:

Section 3 (2) which states that:

The requisite intent, is an intent to cause a modification of the contents of any computer by so doing:

a) To impair the operation of any computer.

b) To prevent or hinder access to any program or data held in a computer, or

c) To impair the operation of any such program or the reliability of any such data.

Section 3 (3) of the Act states that:

The intent need not be directed at:

a) Any particular computer.

b) Any particular program or data or a program or data of any particular kind,

or
c) Any particular modification or modification of any particular kind

A person found guilty of an offence under Section 3 of the Act can be imprisoned for up to five years and/or an unlimited fine.

Proving the offence

To prove that an offence has been committed the following points must be established:

Section 1 the unauthorised access offence

- That the computer performed a function as a consequence of seeking or gaining access.

- That the access was unauthorised.

- That the person concerned knew that the access was unauthorised.

To prove the unauthorised access has taken place it will be necessary for the computer system to have an access control system with secure log which will record all significant events.

The log can be used to prove that access was attempted, or successfully made, from a particular workstation at a certain time.
Section 2 the ulterior intent offence

- That the computer performed a function as a consequence of seeking or gaining access.

- That the access was unauthorised.

- That the person concerned knew that the access was unauthorised.

- That the access was a preliminary to the commission or facilitation of a serious other offence.

Section 3 the unauthorised modification offence

- That modification to computer material was, or would have been caused.

- That the person concerned knew that the modification was unauthorised.

- That the intention behind the modification as to impair the operation of the computer in some way.

The proof of unauthorised modification will be assisted if the time at which this took place can be established. Backups and printouts that are taken on a regular basis will be of assistance here. The access control system should record when data is accessed, when it is backed up and when it is updated.

All those using the computer system should be aware of the limits set for them to make modifications to data and programs.
# 12.3. Appendix C – Classification of Security breaches

<table>
<thead>
<tr>
<th>Type of Effect</th>
<th>Departmental Embarrassment</th>
<th>Personal Safety</th>
<th>Personal Privacy Infringement</th>
<th>Failure to meet Legal Obligations</th>
<th>Commercial Confidentiality Loss (£)</th>
<th>Financial Loss</th>
<th>Disruption to Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insignificant</td>
<td>Contained within Department or Division</td>
<td>Minor injury to individual</td>
<td>Isolated personal detail revealed</td>
<td>Civil suit, &lt;£10K damages</td>
<td>Up to £10K</td>
<td>Up to £10K</td>
<td>Up to £10K</td>
</tr>
<tr>
<td>Minor</td>
<td>Contained within Authority/CCG or NHS</td>
<td>Minor injury to several people</td>
<td>Isolated personal detail compromised</td>
<td>Civil suit, &lt;£10K Small fine, &lt;£10K</td>
<td>£10K to £100K</td>
<td>£10K to £100K</td>
<td>£10K to £100K</td>
</tr>
<tr>
<td>Significant</td>
<td>Local public or press interested and/or Parliamentary Question raised</td>
<td>Major injury to individual</td>
<td>Several personal details revealed</td>
<td>Large fine (above £10K)</td>
<td>£100K to £500K</td>
<td>£100K to £500K</td>
<td>£100K to £500K</td>
</tr>
<tr>
<td>Major</td>
<td>National public or press aware Commons debate</td>
<td>Major injury to several people. Death of individual</td>
<td>Several personal details compromised</td>
<td>Custodial sentence imposed</td>
<td>£500K to £1 million</td>
<td>£500K to £1 million</td>
<td>£500K to £1 million</td>
</tr>
<tr>
<td>Acute</td>
<td>Minister forced to resign. No confidence motion against Government</td>
<td>Death of several people</td>
<td>All personal details revealed and/or compromised</td>
<td>Multiple civil or criminal suits</td>
<td>Above £1 million</td>
<td>Above £1 million</td>
<td>Above £1 million</td>
</tr>
</tbody>
</table>
## 12.4. Appendix D – Incident Classification Table

### INCIDENT CLASSIFICATION TABLE

### NHS HEALTH RISK MATRIX

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Certain</th>
<th>Likely</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td><strong>Likelihood</strong></td>
<td><strong>5</strong> (Moderate)</td>
<td><strong>4</strong> (Moderate)</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>8</td>
</tr>
<tr>
<td><strong>Likelihood</strong></td>
<td><strong>10</strong> (Significant)</td>
<td><strong>8</strong> (Significant)</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>12</td>
</tr>
<tr>
<td><strong>Likelihood</strong></td>
<td><strong>15</strong> (High)</td>
<td><strong>12</strong> (Significant)</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>16</td>
</tr>
<tr>
<td><strong>Likelihood</strong></td>
<td><strong>20</strong> (High)</td>
<td><strong>16</strong> (High)</td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>20</td>
</tr>
<tr>
<td><strong>Likelihood</strong></td>
<td><strong>25</strong> (High)</td>
<td><strong>20</strong> (High)</td>
</tr>
<tr>
<td>Risk Matrix</td>
<td>Moderate</td>
<td>Unlikely</td>
</tr>
<tr>
<td>-------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>Minor</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Moderate</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Serious</td>
<td>Significant</td>
<td>Significant</td>
</tr>
<tr>
<td>Major</td>
<td>Significant</td>
<td>Significant</td>
</tr>
<tr>
<td>Critical</td>
<td>High</td>
<td>Significant</td>
</tr>
</tbody>
</table>

**Risk Matrix**

- **Low**
- **Moderate**
- **Significant**
- **High**

**Consequence**
12.5. Appendix E – Request for computer Access

REQUEST FOR COMPUTER ACCESS

Available on request from the IT Helpdesk
## 12.6. Appendix F - Definitions / Glossary of terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUP</td>
<td>Acceptable User Policy</td>
</tr>
<tr>
<td>HR</td>
<td>Human Resources</td>
</tr>
<tr>
<td>IT Services</td>
<td>Informatics IT Services</td>
</tr>
</tbody>
</table>
| PID       | Personable Identifiable Data  
or  
Patient Identifiable Data |
| CCG       | Within this document CCG refers to Walsall Clinical Commissioning Group |
| Escrow agreements | Source code escrow is the deposit of the source code of software with a third party escrow agent. Escrow is typically requested by a party licensing software (the licensee), to ensure maintenance of the software. The software source code is released to the licensee if the licensor files for bankruptcy or otherwise fails to maintain and update the software as promised in the software license agreement. |
| uTorrent | Software used to download files from the BitTorrent network. Typically files downloaded are pirated. |
12.7. Appendix G – Blank

Intentionally left blank
12.8. Appendix H – Email disclaimer clause

CCG EMAIL DISCLAIMER CLAUSE

Walsall CCG

Any views expressed in this message are those of the individual sender, except where the sender specifically states them to be the views of either of the above organisations.

This message is confidential and may contain privileged information intended only for the addressee and must not be copied or delivered or its contents disclosed to anyone other than the addressee. If you have received this e-mail in error please notify us immediately by e-mail returning the original message to the sender.

Walsall CCG reserves the right to monitor, intercept and (where appropriate) read all incoming and outgoing communications. By replying to this message you are taken as being aware of and giving consent to such monitoring, interception and reading.
CONFIDENTIALITY UNDERTAKING

Walsall Clinical Commissioning Group

Direct Line

Fax

10 August 2016

CONFIDENTIAL

Dear Sir

Re: Confidentiality Undertaking

We are writing to you in relation to the [proposed project idea and the related project information] (“Project”), to confirm the basis on which you, [name of recipient], will be given access to certain Confidential Information relating to the Project by Walsall CCG (“CCG”) for the purpose of evaluating the Project or for the purpose of carrying out any work in relation to the Project (“Purpose”).

In this letter the information that the CCG will disclose to you in relation to the Project, which may include ‘personal data’, sensitive personal data’ (as defined by Section 1(i) and Section 2 of the Data Protection Act 1998 respectively) and medical records, whether orally or in written or machine readable form, (but which does not include any information: (i) which is publicly known or becomes publicly known other than by a breach of this letter; (ii) which, when it was disclosed to you, was already known to you; or (iii) which, after being disclosed to you, is disclosed to you again by a third party at liberty to disclose it) is referred to as the “Confidential Information”.
In consideration of the CCG disclosing the Confidential Information to you, you undertake in relation to the Project, the Purpose and the Confidential Information that you will:

(a) not use any of the Confidential Information, except as expressly permitted by this letter;

(b) not disclose to any other person any of the Confidential Information, except as expressly permitted by this letter; and

(c) only disclose the Confidential Information:

   (i) when required to do so by law or any regulatory authority; and

   (ii) to those of your personnel (including any of your employees, advisors, agents or contractors) whose duties reasonably require such disclosure, on condition that you ensure that each person to whom such disclosure is made is informed of the obligations of confidentiality contained within this letter.

You may not disclose the terms of this letter to any other person, except to your (or any of your parent companies’) employees, contractors, directors, agents or advisers whose duties reasonably require such disclosure and on the conditions referred to in paragraph C (ii).

You may take only such copies of the Confidential Information as are reasonably necessary for the conduct of the Purpose and, immediately upon the CCGs written request, return to the CCG (and procure the return to the CCG by any third party to whom you have disclosed any Confidential Information) or otherwise destroy (or procure the destruction) of all or any of the documents or other material containing or embodying the Confidential Information together with all copies thereof including any reports or analyses or other documents which contain or refer to the Confidential Information.

You agree to promptly notify the CCG, as soon as practicable and where legitimate to do so, if you are required to disclose any Confidential Information under paragraph C (i) before it is disclosed and
to co-operate with the CCG regarding the manner, scope or timing of such disclosure or any action which the CCG may take to challenge the validity of such requirement,

Furthermore, you agree that you shall, having due consideration for the nature of the Confidential Information and the technological measures reasonably available, maintain adequate policies and procedures to ensure that the Confidential Information is kept secure. You further agree to indemnify the CCG against all actions, demands, costs, charges and expenses (including reasonable legal costs) arising from or incurred by the CCG as a result of your breach of this obligation.

You acknowledge that: the Confidential Information is highly confidential and sensitive; that any disclosure or use of the Confidential Information may be highly damaging to the CCGs business and interests; that damages alone would not be an adequate remedy for any breach of your obligation of confidentiality; and that the CCG will, in addition to any other remedy that may be available to it in law, be entitled to obtain injunctive relief against the actual or threatened breach of this agreement without the necessity of proving actual or potential damage.

You also acknowledged that the CCG gives no warranty and makes no representation as to the accuracy or completeness of any of the Confidential Information or as to the reasonableness of any assumptions on which it is based and you agree that the CCG has no liability to you or to any of your directors, employees, advisers or agents resulting from your use of the Confidential Information.

This letter shall not constitute a commitment by any person to supply any Confidential Information or enter into any transaction in relation to the Project. Except as expressly stated, nothing in this letter shall be construed to transfer to you any rights in respect of the Confidential Information or to grant to you any licence.

Nothing in this agreement shall confer on any third party any benefits under the provisions of the Contracts (Rights of Third Parties) Act 1999.

The agreement constituted by the exchange of copies of this letter shall be construed in accordance with English law and shall be subject to the non-exclusive jurisdiction of the English Courts.
Please confirm your understanding and acceptance of the foregoing by signing and returning to the CCG the enclosed copy of this letter.

Yours faithfully,

Departmental Manager

Duly authorised for and on behalf of Walsall CCG

I agree to the foregoing

........................................... ...........................................

[Name] [Date]

...........................................

(Position)

Duly authorised for and on behalf of

[Name of recipient] Limited
Organisations Covered

Approval

The Information Executive Group consisting of a cross section of the management and approves the IT Projects on behalf of the CCG. It also supports the implementation of them through appropriate commitment and adequate resourcing.

Extent of Ex Closure of Information

In order to ensure that no information is made public that could aid anyone with a malicious intent to circumvent security measures, attempt to gain access to, damage, or steal any of the CCG systems or equipment, certain information will not be made available in this document.

Independent Review

The implementation of the IM&T Policies will be reviewed both by internal and external auditors to ensure that adequate controls exist and are enforced to safeguard the CCG assets (equipment or data).

Internal Audit

Internal audit will include within audit plans a review of compliance with the CCG IM&T Policies. Reviews will include computer systems, site installations and data storage facilities.

Following any review a report will be produced which details:

- the degree of compliance with the CCG IM&T Policies.
- any security breaches and incidents of a significant nature.
The auditors' program of work and review of security arrangements will form the basis of any audit assurances provided to external users of the computer facilities.
Specialist Advice

Where required the IT Operations Manager will seek specialist advice from internal or external advisors on information security and advise the CCG accordingly.

Cooperation between organisations

Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators NHS bodies shall be maintained.

Review and evaluation

The policies shall be reviewed regularly to ensure best practise and appropriateness are maintained.

Purpose

It is essential that all information processing systems in the health care environment are protected to an adequate level from events which may jeopardise health care activities. These events will include accidents as well as behaviour deliberately designed to cause difficulties. The purpose of documented IM&T policies is to preserve:-

- Confidentiality data access is confined to those with specified authority to view the data.
- Integrity all system assets are operating correctly according to specification and in the way the current user believes them to be operating.
- Availability information is delivered to right person, when it is needed.
12.10. Appendix J – Good practice in: Mobile Computing

Good Practice In: Mobile Computing

The secure use of laptops, PDAs and other mobile devices

Contacts

These guidelines are intended to complement, but not replace the CCGs formal policies and procedures regarding Information Security.

The latest Information Security documents, policies and leaflets are available for download from the CCGs internal Intranet site.

If you have questions regarding the contents of this leaflet please contact:

IT Helpdesk

Remember

DO

- Read and understand your organisations information security policy and procedures.
- Make sure that your devices are physically secure when unattended.
Keep the information you have on your device to a minimum and make sure that it is backed up in accordance with your organisation's policy.

Encrypt devices and removable media that contain patient or sensitive information.

Ensure patient data that is sent to/from your device is encrypted.

Immediately report any actual or suspected loss, theft, or unauthorised access/disclosure.

DON'T

- Leave your mobile devices unattended
- Leave them in your car, even for a short period
- Hold more information than is necessary
- Carry your device and any access tokens in the same bags
- Share passwords or access tokens
Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents
1. Introduction
1.1 Matthew Swindells’ letter of the 29 February 2008 (Gateway 9571) included guidance on the process for reporting Information Governance (IG) Serious Untoward Incidents and assessing their severity. This is included at Appendix A.

1.2 The definition of an IG SUI given at paragraph 2 of Appendix A is:

Any incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals should be considered as serious.

The above definition applies irrespective of the media involved and includes both loss of electronic media and paper records.

1.3 Experience of reporting and managing IG SUIs has indicated the need for additional guidance, support and clarification of the criteria to be used when evaluating IG SUIs. This guidance has been approved by all SHA IG leads and the DH Digital Information Policy Team. Particular thanks are owed to Clive Thomas, South Central SHA, as the principal author of this document.

2. Purpose of this Checklist

2.1 This checklist should be used in conjunction with the previously provided national guidance on the management of Serious Untoward Incidents and any local guidance on SUIs provided by your SHA. The intention is to ensure that:

- the management of IG SUIs conforms to the processes and procedures set out for managing all Serious Untoward Incidents;
- there is a consistent approach to evaluating IG SUIs;
- early reports of IG SUIs are sufficient to decide appropriate escalation, notification and communication to interested parties;
- appropriate action is taken to prevent damage to patients, staff and the reputation of the NHS;
- all aspects of a SUI are fully explored and ‘lessons learned’ are identified and communicated;
- and appropriate corrective action is taken to prevent recurrence.

2.2 The checklist should be used by all staff involved in managing an IG SUI.

2.3 It is important to note that much of this checklist will be applicable to ‘near misses. Staff should be encouraged to report IG SUI “near misses” and the opportunity taken to identify and disseminate the ‘lessons learnt’.
2.4 All staff should know to whom they should report and escalate suspected or actual IG SUIs.

2.5 All organisations should already have in place an Incident Response Plan (IRP) covering Disaster Recovery, Business Continuity and the development of effective Communications Plans. It is recommended that this checklist is incorporated into the IRP.
2.6 PCTs will be responsible for performance managing the investigation of SUIs in their main providers. Where the SUI takes place in a PCT, the SHA performance lead will manage the investigation.

2.7 The main parts of the process are:

- Initial reporting
- Managing the incident
- Investigating
- Final reporting
Potential loss of Person Identifiable Data Identified

Make initial assessment and provide ‘early warnings’ if appropriate

Initiate Incident Response Plan

Was the loss Person Identifiable Data

Yes

Initiate Incident Response Plan

Level 1 or above

No

Manage locally

Yes

Report on STEIS/ update STEIS

Level 3 or above

Yes

SHA to escalate to DH Business Unit Organisation to notify Information Commissioner

Review SUI Level in light of findings

Investigation

Final Report and lessons learnt

Close Incident Publish on website in accordance with local procedures

Not a SUI

No

Yes
3. Initial Reporting of Serious Untoward Incidents

3.1 Suspected incidents

Initial information is often sparse and it may be uncertain whether a SUI has actually taken place. Suspected incidents and ‘near misses’ should be reported as SUIs as lessons can often be learnt from them and they can be closed when the full facts are known.

3.2 Early notification

Where it is suspected that an IG SUI has taken place, it is good practice to informally notify key staff (Chief Executive, Senior Information Risk Owner, Caldicott Guardian, other Directors, PCT, SHA, DH, etc.) as an ‘early warning’ to ensure that they are in a position to respond to enquiries from third parties and to avoid ‘surprises’. Each organisation needs to determine its own notification priorities.

3.3 Reporting incidents – STEIS will be used for reporting all SUIs and an initial report should be made as soon as possible and no later than 24 hours of the incident or first becoming aware of the incident. Further information will become available as the investigation takes place and STEIS should be regularly updated as appropriate.

3.4 The PCT monitors STEIS and will therefore be aware of all IG SUIs (although please note 3.2 concerning early notification).

3.5 Complete the information required for STEIS.

Ensure that the following are included in the report:

• Date, time and location of the incident

• Type of Incident: “Confidential Information Leak” (NB this may be subject to change as improvements to STEIS data incident reporting are being pursued)
• Contact details for local incident manager

• Confirmation that appropriate and documented incident management procedures are being followed and that disciplinary action will be invoked where appropriate following the investigation

• Description of what happened
  
  Theft, accidental loss, inappropriate disclosure, procedural failure etc.
  The number of patients/staff (individual data subjects) involved
  The number of records involved
  The media (paper, electronic) of the records
  If electronic media, whether encrypted or not
  The type of record or data involved and sensitivity

☐ Whether the SUI is in the public domain

• Whether the media (press etc.) are involved or there is a potential for media interest
• Whether the SUI could damage the reputation of an individual, a work-team, an organisation or the NHS as a whole

• Whether there are legal implications for the CCG

• Initial assessment of level of SUI (see table at Appendix A and 4.2 “Assessing the Incident Level”).

• Whether the following have been notified (formally or informally):

  - Data subjects
  - Caldicott Guardian
  - Senior Information Risk Owner
  - Chief Executive
  - Accounting Officer
  - Information Commissioner for SUI level 3 and above
  - Police, Counter Fraud Branch, etc
  - PCT
Immediate action taken, including whether any staff have been suspended pending the results of the investigation.

Whether the incident is externally reportable: for IG SUIs level 3 and above, local organisations should inform the Information Commissioner once the initial facts are known. The SHA will escalate to DH NHS Business Unit and Media Handling teams. The information that will be needed by the DH is provided in checklist form at Appendix B.

4 Managing the incident

- Identify who is responsible for managing the incident and coordinating separate but related incidents
- Identify who is responsible for the investigation and performance management
- Identify expected outcomes
- Identify stakeholders
- Develop and implement an appropriate communications plan
- Preserve evidence
- Investigate the incident (below)
- Institute formal documentation – this must incorporate version control and configuration management
- Maintain an audit trail of events and evidence supporting decisions taken during the incident
- Where appropriate inform the Information Commissioner (SUI level 3 and above)

Escalate as appropriate (PCT, SHA, SHA to DH Business Unit)

- Inform data subjects (patients, staff)

- Identify and manage consequent risks of the incident (these may be IG-related or involve risks to patient safety, continuity of treatment etc.)

- Identify and manage consequent risks of the incident (these may be IG-related or involve risks to patient safety or continuity of treatment etc.)
• Institute recovery actions

• Invoke organisations disciplinary procedure as appropriate and document the reasons where it is decided not to take action where such action may be viewed as relevant by external parties

• Institute appropriate counter-measures to prevent recurrence

• Identify risks and issues that, whilst not ‘in scope’ of the incident, are appropriate for separate follow-up and action

4 Investigating the incident

4.1 Note that national guidance / requirements are expected on forensic preservation of evidence relating to IG incidents

Appoint investigating officer

Engage appropriate specialist help (IG, IT, Security, Records Management)

Where across organisational boundaries coordinate investigations (and incident management)

Investigate – carry out a Root Cause Analysis

IDT, RCA and report writing and although they need a small of flexibility in order to reflect IG rather than patient safety issues they provide a good structure for investigating and reporting IG incidents).

Organisations should be aware of rules of evidence, interviews, preservation of evidence,
suspending staff, etc.

Document investigation and findings

Ensure that content is reviewed with sources for accuracy

Identify lessons learnt

4.2 Assessing the incident level

Although the primary factors for assessing the severity level are the numbers of individual data
subjects affected, the potential for media interest, and the potential for reputational damage, other
factors may indicate that a higher rating is warranted, for example the potential for litigation or
significant distress or damage to the data subject(s). As more information becomes available, the SUI
level should be re-assessed.

Where the numbers of individuals that are potentially impacted by an incident are unknown, a
sensible view of the likely worst case should inform the assessment of the SUI level. When more
accurate information is determined the level should be revised as quickly as possible and all key
bodies notified.

Where the level of likely media interest is initially assessed as minor but this assessment changes
due to circumstances (e.g. a relevant FOI request or specific journalistic interest) the SUI level should
be revised as quickly as possible and all key bodies notified. Note that informing data subjects is
likely to put an incident into the public/media domain.

5 Final Reporting and Closure of the incident

Set target timescale for completing investigation and finalising reports
Produce report as per NPSA template  
Report reviewed by appropriate persons or appraisal group.  
Sign-off of report – Investigating Officer and CE if serious enough  
Send to the relevant persons and/or committee.  
Identify who is responsible for disseminating lessons learnt  
Closure of SUI – only when all aspects, including any disciplinary  
action taken against staff, are settled.  
Update STEIS  
Where the SUI has been escalated to DH Business Unit notify them,  
of the closure.  
Log SUI details for incorporation in end of year reports by  
Accountable Officer (see Appendix C)  
Publish on CCG/SHA website as appropriate

Appendix A

DoH Guidance 20th Feb 2008 Gateway 9571.

1. Purpose of This Document

It is essential that all serious untoward incidents that occur in CCGs are reported appropriately and handled effectively. This document covers the reporting arrangements and describes the actions that need to be taken in terms of communication and follow up when a serious untoward incident
occurs. CCGs should ensure that any existing policies for dealing with Serious Untoward Incidents are updated to reflect these arrangements.

2. Definition of a Serious Untoward Incident in relation to Personal Identifiable Data

There is no simple definition of a serious incident. What may at first appear to be of minor importance may, on further investigation, be found to be serious and vice versa. **As a guide, any incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals should be considered as serious.**

The above definition applies irrespective of the media involved and includes both loss of electronic media and paper records.

3. Immediate response to Serious Untoward Incident

CCGs should have robust policies in place to ensure that appropriate senior staff are notified immediately of all incidents involving data loss or breaches of confidentiality.

Where incidents occur out of hours, CCGs should have arrangements in place to ensure on-call Directors or other nominated individuals are informed of the incident and take action to inform the appropriate contacts.

4. Assessing the Severity of the Incident

The immediate response to the incident and the escalation process for reporting and investigating this will vary according to the severity of the incident.

Risk assessment methods commonly categorise incidents according to the likely consequences, with the most serious being categorised as a 5, e.g. an incident should be categorised at the highest level that applies when considering the characteristics and risks of the incident.

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>No significant reflection on any individual or body</td>
<td>Damage to an individuals reputation. Possible media interest, e.g. celebrity involved</td>
<td>Damage to a teams reputation. Some local media interest that may not go public</td>
<td>Damage to a services reputation/ Low key local media coverage.</td>
<td>Damage to an organisation’s reputation/ Local media coverage.</td>
<td>Damage to NHS reputation/ National media coverage.</td>
</tr>
<tr>
<td>Media interest very unlikely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minor breach of confidentiality. Only a single individual affected</td>
<td>Potentially serious breach. Less than 5 people affected or risk assessed as low, e.g. files were encrypted</td>
<td>Serious potential breach &amp; risk assessed high e.g. unencrypted clinical records lost. Up to 20 people affected</td>
<td>Serious breach of confidentiality e.g. up to 100 people affected</td>
<td>Serious breach with potential for ID theft or over 1000 people affected</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
</tbody>
</table>

### 5. Reporting to the SHA

The CCG should report the SUI, i.e. all incidents rated as 1 – 5, to the SHA through the usual SUI process. The following information should be provided in each case:

- A short description of what happened, including the actions taken and whether the incident has been resolved
- Details of how the information was held: paper, memory stick, disc, laptop etc
- Details of any safeguards such as encryption that would mitigate risk
- Details of the number of individuals whose information is at risk
- Details of the type of information: demographic, clinical, bank details etc
Whether a) the individuals concerned have been informed, b) a decision has been taken not to inform or c) this has not yet been decided

Whether a) the Information Commissioner has been informed, b) a decision has been taken not to inform or c) this has not yet been decided

Whether the SUI is in the public domain and the extent of any media interest and/or publication

Reporting to the SHA should be undertaken as soon as practically possible (and no later than 24 hours of the incident during the working week).

If there is any doubt as to whether or not an incident meets the SUI reporting criteria, the CCGs’ Risk Manager or the SHA should be contacted by telephone for advice. Early information, no matter how brief, is better than full information that is too late.

The CCG should keep the SHA informed of any significant developments in internal/external investigations, as appropriate. The SHA should continue to keep a watching brief on developments including following up further details/outcomes of the incident.

The CCGs communications team should contact the SHAs Communications team immediately if there is the possibility of adverse media coverage in order to agree a media handling strategy. Where necessary, the SHA Communications team will brief the Department of Health Media Centre.

6. Reporting to the Department of Health

The SHA will be responsible for notifying the DH of any category 3-5 incident reported by forwarding details to the appropriate dedicated mailbox established within the DH. Incidents should be notified to DH comms only if only the lighter shaded risk areas in the top two rows in the table apply and to both DH Comms and the NHS Business Unit if the significant risks in the darker shaded area at the bottom right of the table apply. This latter, most serious category is the one that should be referenced as a nationally reported SUI. Those reported to DH Comms alone should be referred to as a comms alert derived from a local SUI. Once an incident has been reported to DH any subsequent details that emerge relating to the investigation and resolution of the incident should also be supplied.
The DH will review the incident and determine the need to brief Ministers and/or take other action at a national level.

7. Reporting to the Information Commissioner or other Bodies.

The Information Commissioner should be informed of all Category 3-5 incidents. The decision to inform any other bodies will also be taken, dependent upon the circumstances of the incident, e.g. where this involves risks to the personal safety of patients, the National Patient Safety Agency (NPSA) may also need to be informed.

8. Informing Patients

Consideration should always be given to informing patients when person identifiable information about them has been lost or inappropriately placed in the public domain. Where there is any risk of identity theft it is strongly recommended that this done.
Appendix B

Information required by the Department of Health for category 3+ SUIs

<table>
<thead>
<tr>
<th>Unique SUI Reference:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial assessment of level of SUI (1-5):</td>
<td></td>
</tr>
<tr>
<td>SHA Responsible:</td>
<td></td>
</tr>
<tr>
<td>Local Organisation(s) involved:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Date, time and location of the incident</td>
</tr>
<tr>
<td>02</td>
<td>Confirmation that DH guidelines for incident management are being followed and that disciplinary action will be invoked if appropriate</td>
</tr>
<tr>
<td>03</td>
<td>Description of what happened: Theft, accidental loss, inappropriate disclosure, procedural failure etc.</td>
</tr>
<tr>
<td>04</td>
<td>The number of patients/ staff (individual data subjects) data involved and/or the number of records</td>
</tr>
<tr>
<td>05</td>
<td>The type of record or data involved and sensitivity</td>
</tr>
<tr>
<td></td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>06</td>
<td>The media (paper, electronic, tape) of the records</td>
</tr>
<tr>
<td>07</td>
<td>If electronic media, whether encrypted or not</td>
</tr>
<tr>
<td>08</td>
<td>Whether the SUI is in the public domain and whether the media (press etc.)</td>
</tr>
<tr>
<td></td>
<td>are involved or there is a potential for media interest</td>
</tr>
<tr>
<td>09</td>
<td>Whether the reputation of an individual, team, an organisation or the NHS</td>
</tr>
<tr>
<td></td>
<td>as a whole is at risk and whether there are legal implications</td>
</tr>
<tr>
<td>10</td>
<td>Whether the Information Commissioner has been or will be notified and if</td>
</tr>
<tr>
<td></td>
<td>not why not</td>
</tr>
<tr>
<td>11</td>
<td>Whether the data subjects have been or will be notified and if not why not</td>
</tr>
<tr>
<td>12</td>
<td>Whether the police have been involved</td>
</tr>
<tr>
<td>13</td>
<td>Immediate action taken, including whether any staff have been suspended</td>
</tr>
<tr>
<td></td>
<td>pending the results of the investigation</td>
</tr>
<tr>
<td>14</td>
<td>Whether there are any consequent risks of the incident (e.g. patient safety,</td>
</tr>
<tr>
<td></td>
<td>continuity of treatment etc.) and how these will be managed</td>
</tr>
<tr>
<td>15</td>
<td>What steps have been or will be taken to recover records/data (if applicable)</td>
</tr>
<tr>
<td>16</td>
<td>What lessons have been learned from the incident and how will recurrence</td>
</tr>
<tr>
<td></td>
<td>be prevented</td>
</tr>
<tr>
<td>17</td>
<td>Whether, and to what degree, any member of staff has been disciplined - if</td>
</tr>
<tr>
<td></td>
<td>not appropriate why?</td>
</tr>
<tr>
<td>18</td>
<td>Closure of SUI – only when all aspects, including any disciplinary action</td>
</tr>
<tr>
<td></td>
<td>taken against staff, are settled.</td>
</tr>
</tbody>
</table>

Notes:
Appendix C

Publishing details of SUIs in annual reports and Statements of Internal Control

Principles

The reporting of personal data related incidents in the Annual Report should observe the principles listed below. The principles support consistency in reporting standards across Organisations while allowing for existing commitments in individual cases.

a) You must ensure that information provided on personal data related incidents is complete, reliable and accurate.

b) You should review all public statements you have made, particularly in response to requests under the Freedom of Information Act 2000, to ensure that coverage of personal data related incidents in your report is consistent with any assurances given.

c) You should consider whether the exemptions in the Freedom of Information Act 2000 or any other UK information legislation apply to any details of a reported incident or whether the incident is unsuitable for inclusion in the report for any other reason (for example, the incident is sub judice and therefore cannot be reported publicly pending the outcome of legal proceedings).

d) Please note that the loss or theft of removable media (including laptops, removable discs, CDs, USB memory sticks, PDAs and media card formats) upon which data has been encrypted to the approved standard, is not a Serious Untoward Incident unless you have reason to believe that the protections have been broken or were improperly applied.

Content to be included in Annual Reports

Incidents classified at a severity rating of 3-5 (see Appendix A) are those that should be captured as Serious Untoward Incidents and should be reported to SHAs and to the Information Commissioner. These incidents need to be detailed individually in the annual
<table>
<thead>
<tr>
<th>Date of incident (month)</th>
<th>Nature of incident</th>
<th>Nature of data involved</th>
<th>Number of people potentially affected</th>
<th>Notification steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan</td>
<td>FOR EXAMPLE</td>
<td>Name; address; NHS No</td>
<td>1,500</td>
<td>Individuals notified by post</td>
</tr>
</tbody>
</table>

Further action on information risk

The [organisation] will continue to monitor and assess its information risks, in light of the events noted above, in order to identify and address any weaknesses and ensure continuous improvement of its systems.

The member of staff responsible for this incident has been dismissed.

Notes to producing Table 1

Nature of the incident

Select one of:

a) Loss of (insert from category list below) from secured NHS premises

b) Theft of (insert from category list below) from secured NHS premises

c) Loss of (insert from category list below) from outside secured NHS premises (including, for example, post, courier, loss by a contractor or third party supplier)

d) Theft of (insert from category list below) from outside secured NHS premises (including, for example, theft from employee home or car)

e) Insecure disposal of (insert from category list below) (including, for example, sale of computers with unwiped hard drives, disposal of unshredded paper documents)

f) Unauthorised disclosure (including, for example, criminal, negligent or inappropriate use of an
information system or information asset by a staff member, contractor or third party supplier, resulting in disclosure; disclosure as a result of software or systems failure)

g) Other

<table>
<thead>
<tr>
<th>Category List</th>
</tr>
</thead>
<tbody>
<tr>
<td>i) inadequately protected PC(s), laptop(s) and remote device(s) <em>(including, for example, PDAs, mobile telephones, Blackberrys)</em></td>
</tr>
<tr>
<td>ii. inadequately protected electronic storage device(s) <em>(including, for example, USB devices, discs, CD ROM, microfilm)</em></td>
</tr>
<tr>
<td>iii. inadequately protected electronic back-up device(s) <em>(including, for example, tapes)</em></td>
</tr>
<tr>
<td>iv. paper document(s)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Nature of data involved</th>
</tr>
</thead>
</table>
| A list of data elements *(e.g. name, address, NHS number)*.

<table>
<thead>
<tr>
<th>Number of people potentially affected</th>
</tr>
</thead>
</table>
| An estimate should be provided if no precise figure can be given.

<table>
<thead>
<tr>
<th>Notification steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individuals notified by post* / email* / telephone* <em>(delete as appropriate)</em></td>
</tr>
<tr>
<td>Police* / law enforcement agencies* notified <em>(delete as appropriate)</em></td>
</tr>
<tr>
<td>Media release</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Further action on information risk</th>
</tr>
</thead>
</table>
| A summary of any disciplinary action taken as a result of the incidents should also be included.

Incidents classified at lower severity ratings
Incidents classified at a severity rating of 1-2 should be aggregated and reported in the annual report in the format provided as Table 2 below.

Incidents rated at a severity rating of 0 need not be reflected in annual reports.

Table 2

<table>
<thead>
<tr>
<th>Category</th>
<th>Nature of incident</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Loss/theft of inadequately protected electronic equipment, devices or paper documents from secured NHS premises</td>
<td></td>
</tr>
<tr>
<td>II</td>
<td>Loss/theft of inadequately protected electronic equipment, devices or paper documents from outside secured NHS premises</td>
<td></td>
</tr>
<tr>
<td>III</td>
<td>Insecure disposal of inadequately protected electronic equipment, devices or paper documents</td>
<td></td>
</tr>
<tr>
<td>IV</td>
<td>Unauthorised disclosure</td>
<td></td>
</tr>
<tr>
<td>V</td>
<td>Other</td>
<td></td>
</tr>
</tbody>
</table>

SIC Guidance

It is important to remember that an organisation's assets include information as well as more tangible parts of the estate. Information may have limited financial value on the balance sheet but it must be managed appropriately and securely. All information used for operational purposes and financial reporting purposes needs to be encompassed and evidence maintained of effective information governance processes and procedures with risk based and proportionate safeguards. Personal and other sensitive information clearly require particularly strong safeguards. The Accountable Officer and the board need comprehensive and reliable assurance from managers, internal audit and other assurance providers that appropriate controls are in place and that risks, including information and reporting risks, are being managed effectively.
The SIC should, in the description of the risk and control framework, explicitly include how risks to information are being managed and controlled as part of this process. This can be done for example by referencing specific work undertaken by your organisation and by reference to your organisation’s use of the Information Governance Toolkit. The SIC will then be reflected formally in your Annual report.

Any incidence of a Serious Untoward Incident (as described in Appendix A) should be reported in the SIC as a significant control issue. For the avoidance of doubt these are those incidents with a severity rating of 3, 4 or 5.
12.12. Appendix L – Smartcard good practice

You must not leave a computer that is logged in unattended unless it has been secured.

You are responsible for either terminating the session (logging off) when finished or locking the computer when temporarily leaving it unattended.

Make sure your Smartcard is safe and secure at all times and do not leave it inserted in to the keyboard when not in use.

In the event of loss, theft or damage to your Smartcards, or if you suspect someone knows your PIN number, you much contact the IT Helpdesk as soon as possible.

You must also ensure that any suspected or actual breaches of security are reported to the IT Helpdesk.

The Helpdesk extension number is on the Contacts page of this leaflet.

Please contact the IT Helpdesk in case of:

Lost Smartcard
Stolen Smartcard
Damaged Smartcard
PIN changed
Breaches of Security
Breaches of Confidentiality
Any question

The latest Information Security documents, policies are available for download on the CCGs Intranet site.
A full copy of the NHS CRA Acceptable Use Policy is available on the NHS Connecting for Health website at:

www.connectingforhealth.nhs.uk

Information Security

NHS Records Service Smartcard Guidelines
Introduction

Smartcards are required to access the NHS Care Records Service (NHS CRS).

They are used in conjunction with a PIN number, providing an additional layer of security to help prevent unauthorised access to the system and the information held within it.

All users of the NHS CRS must abide by the information in this leaflet which is designed to assist all members of staff with compliance.

Automated systems are used to monitor and record computer activity to audit the effective operation of the systems and for other lawful purposes.

---

Individual users can be identified from the information recorded and this information will be accessed and used to investigate allegations of breaches of security and/or confidentiality.

Smartcard Guidelines

You are personally responsible for ensuring that patient/client information is protected and only used for specified and lawful purposes.

Smartcards are issued to individual members of staff and must only be used by the person whose name is on the card.

Accessing the NHS CRS system using another member of staff’s Smartcard is against the law, even if you are authorised to have access to the information.

All information held in the NHS CRS is confidential and care must be taken by
everyone issued with a Smartcard to keep it secure and protect their PIN against discovery.

Do not discuss the confidential information held on the NHS CRS with people who are not authorised to know it.

You must not access or attempt to access confidential information that has nothing to do with your job e.g. personal and confidential information about your family, friends or colleagues.

All system activity is monitored.

Staff who become patients do not have an automatic right to view their own information.

Any member of staff wishing to view their own records should make a formal application to the organisation holding the records or talk to the people providing their care and treatment.

Do not write down your PIN number without adequate protection e.g. keep in a locked drawer or held password protected on a PDA (Personal Digital Assistant).

Wherever possible site your display screen where the contents cannot be easily read by unauthorised people.
12.13. Appendix M - List of external organisations and companies

Paper Disposal:

Confi-Shred Ltd
UK Customer Services & Operations Centre
Unit 4
Hortonwood 8
Telford
TF1 7GR

Tel: 01952 602730
Tel: 0845 601 7218
Fax: 01952 670987
Web: www.confishred.com/

IT Hardware Disposal:

Northern Computer Recycling Ltd (NCR)
Unit 36
Stella Gill Industrial Estate
Chester-le-Street
Co Durham
12.14. Appendix N  Sample Disposal of Media Record

### Electronic Media Destruction Register

<table>
<thead>
<tr>
<th>Collection</th>
<th>Erasure</th>
<th>Disposal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Type</td>
<td>Qty</td>
<td>Received From Center/Dept</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
<td>---------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This is a controlled form and must be retained for Audit purposes
### Equipment Movement

**IT Installation Date:**

**Job No.:**

**Date:**

<table>
<thead>
<tr>
<th>User</th>
<th>Engineer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact:</td>
<td>Contact:</td>
</tr>
<tr>
<td>Location:</td>
<td>Location:</td>
</tr>
<tr>
<td>Telephone:</td>
<td>Telephone:</td>
</tr>
</tbody>
</table>

**Equipment to be moved:**

<table>
<thead>
<tr>
<th>Asset No.</th>
<th>Item Description</th>
<th>User Name</th>
<th>Old Location</th>
<th>New Location</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**New Location:**

Power Sockets (Estates) [ ]
Network Points (IT) [ ]
Telephone Points (Support Services) [ ]

If any of the above required but not ticked please contact the relevant department to arrange a site visit and/or work to be carried out prior to the move date.

**Other (please use additional sheet if required):**

Fax Machines

Analogue Phones

Please note access will be needed to power sockets/network points/telephone points during the move. Please ensure that these are not blocked by desks and filing cabinets.
### 12.16. Appendix P – Computing equipment movement sheet

**Computing Equipment Movement Sheet**

<table>
<thead>
<tr>
<th>Date / /</th>
<th>Asset Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description**

**Destination Address:**

**Period Off Site**

1. Limited Period
2. Permanently
3. Regular Movement on & off Site
4. Replacement / Repair Item

**Until:** / /

**Reason for Movement**

**REMOVAL AUTHORISATION**

Name of Person Taking item Off Site

Signature of Person Taking Off Site

Date of removal From Site

Name of Person Authorising Removal from Site

Signature of Person Authorising Removal from Site

**RETURN MONITORING**

Name of Person Returning Item to Site

Signature of Person Returning Item to Site

Date of Return To Site / /

Name of Person Accepting Return of Item to Site

Signature of Person Accepting Return of Item to Site
### 12.17. Appendix Q – Approval for Remote Working

The member of staff named below has received express approval to work remotely and has read, understood and agrees to the conditions within the CCG’s policy on remote working.

<table>
<thead>
<tr>
<th>Equipment being used</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong> ..........................................................</td>
</tr>
<tr>
<td><strong>Assed Number</strong> ...........................................................</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name of applicant</th>
</tr>
</thead>
<tbody>
<tr>
<td>………………………</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>………………………</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>………………………</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Line Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>………………………</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>………………………</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>………………………</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Head of Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>………………………</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>………………………</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>………………………</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Line Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>………………………</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>………………………</td>
</tr>
</tbody>
</table>
An approved remote working application should be kept by the member of staff, their line manager with one copy for the personal file and one copy to IT Services Helpdesk.

Access will not be provided until complete form is received by IT Services Helpdesk.