North Hampshire
Clinical Commissioning Group

NHS South, Central and West Commissioning Support Unit

Information Security Policy

As the South, Central & West Commissioning Support Unit (SCW) provides IT networks, equipment and support to North Hampshire CCG, all CCG employees are required to adhere to the CSU IT Services information security policies. The following policy was developed by the CSU IT Services Team and adopted for use by the CCG.

This document can be made available in a range of languages and formats on request to the policy author.

Version:	2.1
Ratified by:	SCW CSU Corporate Governance Assurance Group
Date ratified:	29/11/2016
Name of Responsible Officer/author:	Andy Ferrari – Associate Director of IT Strategy and Planning
Name of responsible committee/individual:	IT Services Senior Leadership Team
Name of executive lead:	Suzanne Tewkesbury – Director of Corporate Development & Performance
Date issued:	09/01/2018
Review date:	25/05/2018
Target audience:	All NHS South, Central and West CSU staff

Document Control Sheet

Title	**IT Services - Information Security Policy**
CCG	All
Version	2.1
Status	Approved – Final
Author	David Walch
Date Created	29.12.2015
Date Last Updated	14/12/2017

History			
Version	Date	Author(s)	Comments
1.0	29/12/2015	David Walch	Version reset & re-write specifically for SCW CSU
1.1a	08/09/2016	Arif Gulzar	Updated policy review date
1.1b	04/10/2016	Arif Gulzar	Policy signed off by Information Governance Steering Group
2.0	29/11/2016	Arif Gulzar	Version reset after ratification from Corporate Governance Assurance Group
2.1	14/12/2017	Arif Gulzar	Extended policy review date to align with GDPR after approval from SCW Information Governance Steering Group

Approval/Sign Off	
Name	Title and contact
Catherine Dampney	CIO
Philip Evans	Associate Director of IT Services

Contents

1 Introduction and Purpose

Information and Cyber Security has critical importance to NHS patient care, information assets and other related business processes. High quality information underpins the delivery of high quality evidence-based healthcare. Without effective security, NHS information assets may become unreliable, may not be accessible when needed, or may be compromised by unauthorised third parties. Information, whether in paper or electronic form, is of high importance to the NHS South, Central and West Commissioning Support Unit (SCW), therefore the organisation must ensure that the information is properly protected and is reliably available.

Information Security is primarily about people but is facilitated by the appropriate use of technology. The business benefits of this policy and associated guidance are:

- Assurance that information is being managed securely and in a consistent and corporate way.
- Assurance that SCW is providing a secure and trusted environment for the management of information used in delivering its business.
- Clarity over the personal responsibilities around information security expected of staff (as defined in the scope) when working on SCW business.
- A strengthened position in the event of any legal action that may be taken against the SCW (assuming the proper application of the policy and compliance with it).
- Demonstration of best practice in Information Security.
- Assurance that information is accessible only to those authorised to have access.

The requirements within this Policy are driven by the Data Protection Act 1998 which is the key piece of legislation covering security and confidentiality of personal information.

2 Scope and Definitions

2.1 Scope

This policy applies to all SCW staff. Compliance and responsibility also extends to those employed by the SCW as contractors, NHS professionals, temporary staff, voluntary organisations and anyone duly authorised to view or work with SCW's information.

All references to Information Security are inclusive of Cyber Security measures.

The purpose of this Information Security Policy is to protect, to a consistently high standard, all information assets, including patient and staff (as defined in the scope) records and other NHS corporate information, from all potentially damaging threats, whether internal or

external, deliberate or accidental. SCW has a legal obligation to ensure that there is adequate provision for the security management of the information resources the organisation owns, controls, or uses. This Information Security Policy forms part of a suite of Information Governance documentation including but not limited to: Information Governance Policy, Data Protection Act Policy, and the Records Management & Lifecycle Policy.

This Information Security Policy covers all forms of information held by the SCW, including but not limited to:

- Information about members of the public and patients
- Non NHS South, Central and West CSU staff on NHS South, Central and West CSU premises
- Staff (as defined in the scope) and Personnel Information
- Organisational, Business and Operational Information

This Information Security Policy applies to all aspects of information handling, including, but not limited to:

- Structured Record Systems – paper and electronic
- Information Recording and Processing Systems – Paper, Electronic, Video, Photographic and Audio Recordings.
- Information Transmission Systems, such as fax, email, portable media, post and telephone.

2.2 Definitions

Asset
Anything that has value to the organisation, its business operations and its continuity.

Authentication
The organisation must ensure that the identity of a subject or resource is the one claimed

Availability
The property of being accessible and usable upon demand by an authorised entity

Business Impact
The result of an information security incident on business functions and the effect that a business interruption might have upon them.

Confidentiality
The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Cyber Security

Information and Cyber Security concerns the comprehensive risk management, protection and resilience of data processing and the digital networks that connect them.

Impact
The result of an information security incident, caused by threat, which affects assets.

Information Assurance
The confidence that information assets will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.

Information Security
The preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability and reliability can also be involved.

Personal Confidential Data and Sensitive Data is where an individual can be identified:

a. from the data, or
b. from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

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 (Data Protection Act 1998)

Staff
All SCW staff, those employed by SCW as contractors, NHS professionals, temporary staff, voluntary organisations and anyone duly authorised to view or work with SCW's information.

3 Process Requirements

This Information Security Policy will achieve a consistent approach to the security management of information throughout NHS South, Central and West CSU, and will aim to deliver continuous business capability, and minimise both the likelihood of occurrence and the impacts of information security incidents.

Security of our information is paramount and the protective measures put in place, must ensure that Information Governance (IG) requirements are satisfied. The aim of this process is maintaining the confidentiality, integrity, and availability of SCW's information. To conform to the Information Security Assurance requirements of Health & Social Care Information Centre IG Toolkit SCW shall:

Maintain the Confidentiality of Personal Information including patient and staff (as defined in the scope) identifiable information by protecting it in accordance with NHS Information Security Code of Practice, Data Protection Act, Caldicott Principles and other legal and regulatory framework criteria.

Ensure the integrity of SCW information by developing, monitoring and maintaining it to a satisfactory level of quality for use within the relevant areas.

Implement the necessary measures to maintain availability of NHS South, Central and West CSU information systems and services. This includes putting in place contingency measures to ensure the minimum of disruption caused to NHS South, Central and West CSU information systems and services.

This Information Security Policy is consistent with and supports NHS South, Central and West CSUs policies and existing methods of working, which take precedence on any specific issue, and is in accordance with NHS national guidance.

3.1 Physical Security

The physical security of SCW information is the responsibility of all staff (as defined in the scope). The protection of both personal and non-personal information is paramount in maintaining confidentiality, and users of SCW information must comply with the suite of Information Governance documentation. This is a local Information Security Policy to protect the information stored, processed and exchanged between SCW and other organisations.

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an appropriate confidentiality clause. Information security expectations of staff shall be included within appropriate job definitions.

Staff shall accept full responsibility for the security of information and information assets which are issued to them, taking necessary precautions to avoid loss, theft or damage. Information should not be left unattended in a public place or left in vehicles either on view, unattended or overnight. In the event of such an incident, Staff must report this immediately to the Information Governance team who will assist with the management of the incident.

All access to confidential and/or sensitive information (whether on paper or electronically) located within SCW property must be controlled through the use of the approved security measures. Advice and guidance can be sought from NHS South, Central and West CSU IG Team or the IT hosted service. Access to information shall be restricted to users who have an authorised business need and access has been approved by the relevant Information Asset Owner (IAO). Other staff responsibilities include ensuring perimeter security by making sure that security doors are closed properly, blinds drawn, and that any door entry codes are changed regularly.

All staff must wear identification badges and individuals not wearing identification in areas which are not for public access should be challenged. Visitors should be met at reception points and accompanied at all times even when leaving the building. Identification badges should be surrendered on termination of contract along with door keys, Smartcards and all other equipment provided by or belonging to SCW.

Portable devices that are intended for use with PCD or sensitive information must be supplied and supported by the CSU. Where it is not practical for contractors or interim staff to obtain approved devices PCD or sensitive information must not be transferred and a suitable device should be sought.

Each team is responsible for holding an information asset register which details the specification, user and location of the asset. IT equipment will be security marked and its serial number should be recorded. It is the responsibility of the area's assigned Data Custodian to update the asset register and submit to the SCW IG Team.

Each team will have a designated Information Asset Owner (IAO) who is responsible for all information held and used by that team

Management of computers and networks shall be controlled through standard documented procedures. Agreed contracts with third party suppliers working for and on behalf of SCW must adhere to CSU policies and procedures.

3.1.1 Protection from Malicious Software

All IT equipment used by SCW staff (as defined in the scope) is protected by countermeasures and management procedures to protect against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation's property without permission from the SCW Associate Director of IT Services or the Cyber Security Manager. Users breaching this requirement may be subject to disciplinary action.

3.1.2 Preventing Information Security Breaches

Each CSU Team is responsible for regularly monitoring the information they hold and use. An annual mapping exercise of information flows in and out of the teams will be undertaken. This exercise will allow any information risks to be identified by each team and appropriate action to mitigate those risks should be taken. It is the responsibility of the IAO to ensure that this takes place.

Protection against unauthorised access or disclosure:
Staff (as defined in the scope) have the responsibility to ensure that information is kept secure at all times by adhering to the following:

- Screens should be locked when unattended even for short periods of time,
- Registration Authority Policy (and procedures)
- Password policy
- Internet and email policies,
- Remote Working and Portable Devices Policy

- Guidance provided on the use of fax, phones and post which can be found within the Safe Haven Policy.
- Disposal of equipment

For the secure transfer of bulk electronic information, secure file transfer function within NHSmail should be used as it has the approved levels of encryption.

SCW will ensure that paper information is secure by following adequate records management procedures and processes. Staff should have access to secure storage areas and if possible, a clear desk routine should be followed. Should a legitimate need arise for local storage or a non-routine transfer of confidential information then a risk assessment must be undertaken first and the justification approved by the Caldicott Guardian and recorded by the line manager. SCW staff must also ensure when moving away from desks that they do not leave person identifiable / sensitive information available for others to view by putting it in a drawer or covering it up.

SCW promotes a 'paperlite' environment through use of electronic devices to transform information to a secure electronic form.

Any non-routine bulk extracts (50+ records) or transfers of particularly confidential or sensitive data must be authorised by the responsible Director or the Information Asset Owner for the work area and may require approval by the Senior Information Risk Owner.

That the integrity and value of the information is maintained: The organisation ensures that staff and contracted individuals are aware and apply the Data Protection Act and Caldicott Principles through their working practices. The SCW Information Governance Team promotes the principles and provides or facilitates training.

That information shall be available to properly authorised personnel as and when it is required: All staff are required to use the guidance contained in the NHS Confidentiality Code of Practice, Care Record Guarantee and the Records Management Code of Practice. The Information Governance suite of policies provides further guidance.

Organisation-wide business continuity plans for information systems are in place: This includes identification and assessment of critical dependencies on SCW information resources. The organisation will implement a business continuity management system (BCMS) that will be aligned to the international standard of best practice (ISO 22301 – Societal Security – Business Continuity Management Systems). Business Impact Analysis will be undertaken in all areas of the organisation.

Business continuity plans will be put into place to ensure the continuity of
prioritised activities in the event of a significant or major incident. The SIRO has a responsibility to ensure that appropriate disaster recovery plans

are in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis.

Relevant Information Security Training and awareness is available to staff via the Health and Social Care Information Centre (HSCIC) Information Governance Training Modules. Additional training needs beyond this will be assessed.

All breaches of information security, actual or suspected, are recorded, and reported using the agreed incident management process for NHS South, Central and West CSU.

3.1.3 Potential or Actual Information Security Breaches

All staff (as defined in the scope) are responsible for ensuring that no potential or actual security breaches occur as a result of their actions. SCW IG Team will investigate all suspected / actual security breaches.

The SCW IG Team and the Risk Management lead must be informed of all security issues in order to ensure that the appropriate investigations are carried out. The SCW Registration Authority (RA) Manager will also receive copies of any Registration Authority related security breaches or incidents.

Depending on the impact of the incident, external organisations such as the NHS England, Health and Social Care Information Centre and the Information Commissioners Office may be informed.

The resulting Root Cause Analysis (RCA) report will specify, details of suspected incident, assets affected or compromised and investigation conducted. Recovery/contingency plans, damage and risk classification and recommendations will be provided.

All incidents will be investigated immediately and reported in a timescale appropriate to the initial risk assessment. Reports and recommendations will be approved and monitored by an appropriate Group within SCW.

3.1.4 Risk

SCW will need to ensure that adequate audit provision is in place to ensure continuing effectiveness of information security management arrangements.

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

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

- The ***Likelihood*** of such a threat occurring.

All staff (as defined in the scope) should consider the risks associated with the computers they use and the information that is held on them, as well as information held in manual records

All staff are responsible for reporting any apparent shortcomings of security measures currently employed to address these risks to the Head of Risk Assurance within SCW.

3.1.5 Information Disposal

Electronic – See ICT disposal policy for more detail
Computer assets must be disposed of in accordance with the ICT Provider disposal of confidential waste procedure. This includes removable computer media, such as tapes and disks.

All data storage devices must be purged of sensitive data before disposal. Where this is not possible, the equipment or media must be destroyed by a technical waste service provider. For further information, please contact the CSU's IT provider.

Paper
Printed matter should be confidentially destroyed using an appropriate method such as shredding. Where SCW has large quantities of confidential waste which need to be disposed of the IG team can help facilitate this through a secure shredding contract.

3.1.6 Security of third party access to NHS Networks

Written agreement must be received from all external contractors and non-NHS parties that they agree to treat all information confidentially and that information will not be disclosed to unauthorised individuals. Such contractors should also sign a declaration that they understand the relevant legislation should they need to access sensitive information stored on a computer system. This declaration is available at Appendix 2

4 Roles and Responsibilities

NHS South, Central and West Commissioning Support Unit Managing Director
SCW's Managing Director has overall responsibility for governance within the organisation. As the accountable officer he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

NHS South, Central and West Commissioning Support Unit Caldicott Guardian
SCW's Caldicott Guardian is seen as the 'conscience' of the organisation regarding the use of personal confidential data. They are responsible for ensuring all personal confidential data is shared in an appropriate and secure manner.

NHS South, Central and West Commissioning Support Unit Senior Information Risk Owner (SIRO)

SCW's Senior Information Risk Owner (SIRO) is responsible for providing leadership on the management of Information Risk and for overseeing the development of an Information Risk Policy. For ensuring the Corporate Risk Management process includes all aspects of Information risk and for ensuring SCW Executive Management Team is adequately briefed on information risk issues. The SCW IG team will support this role.

Cyber Security Manager

The Cyber Security Manager is responsible for the implementation and enforcement of IT security. Regular reports will be submitted to the CSU's IGSG.

Information Asset Owners

The SIRO is supported by the departmental IAOs. The role of IAO is to understand what information is held, what is added and what is removed, who has access and why in their own area. As a result they are able to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of the assets. The organisation has allocated this role to Senior Departmental Heads and/or Managers for each department.

Data Custodians

The Data Custodians within SCW have the responsibility of assisting the IAOs in providing assurance that information risk and the handling of information requirements are managed effectively. Data Custodians should also ensure staff (as defined in the scope) compliance with policies and legislation/principles (Data Protection Act 1998, Common Law Duty of Confidentiality and Caldicott principles).

SCW will ensure that applications to use remote working systems, portable computing and data storage resources, are approved via an agreed process that can be audited.

NHS South, Central and West Commissioning Support Unit Staff

All staff (as defined in the scope), whether permanent, temporary, contracted, or contractors are responsible for ensuring that they are aware of the legal and policy requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.
All staff must abide by this and associated policies and procedures.

All staff should report any suspected breaches of this policy to their line manager or the assigned Data Custodian and the NHS South, Central and West CSU IG team.

All staff must be aware and understand that failure to comply with the rules regulations contained within this policy, may result in disciplinary action.

5 Training

SCW recognises that staff (as defined in the scope) are working to a code of conduct which stresses the importance of appropriate information handling which incorporates statutory, common law and best practice requirements. As Information Governance is a framework drawing these requirements together, it is important that staff receive the appropriate training.

The NHS Operating Framework 'Informatics Planning' requires that the organisation ensures all staff receive annual basic Information Governance training appropriate to their role through the online NHS Information Governance Training Tool or from their IG manager. Managers are responsible for monitoring staff) compliance.

SCW staff will receive an Information Governance staff Handbook on joining the organisation. staff will be required to sign and return a receipt to the SCW IG Team to evidence their compliance.

6 Equality and Diversity

This policy was assessed against SCW Impact Needs Requirement Assessment (INRA) tool to ensure that it does not introduce any unexpected or unwarranted equality and diversity issues this can be seen at appendix 1.

7 Success Criteria/Monitoring of the Effectiveness of the Policy

NHS South, Central and West CSU IT Services Leadership Team is responsible for the approval of this policy. The SCW CSU Corporate Governance Assurance Group will then ratify that approval.

SCW's Senior Information Risk Owner (SIRO), Information Asset Owners and Data Custodians are responsible for the implementation of this policy throughout the organisation.

Regular audits should be undertaken by Data Custodians to ensure that all portable computing and mobile devices issued can be accounted for and that assurance is provided to the Senior Information Risk Owner (SIRO) that identified risks are adequately controlled and managed.

Adherence to this policy will be monitored via investigation and analysis of information security incidents reported via the approved incident management process.

8 Review

The SCW Executive Management Team is responsible for the review of this policy.

9 References and Links to other Documents

Information Governance Policy and Framework

Data Protection Policy
Safe Haven Policy
Information Security Management: NHS Code of Practice
NHS Records Management: Code of Practice
NHS England Information Security Policy
NHS South, Central and West CSU IT security policies

Appendix 1

Analysing the Impact on Equality

1.	**Title of policy/ programme/ framework being analysed** Information Security Policy.
2.	**Please state the aims and objectives of this work and the *intended equality outcomes*. How is this proposal linked to the organisation's business plan and strategic equality objectives?** To provide a framework of guidance to NHS South, Central and West CSU staff (as defined in the scope) regarding the security of Personal Identifiable Data in both paper and electronic form.
3.	**Who is likely to be affected? e.g. staff (as defined in the scope), patients, service users, carers** Staff.
4.	***What evidence do you have of the potential impact (positive and negative)?*** None expected.
4.1	**Disability** (Consider attitudinal, physical and social barriers) No impact
4.2	**Sex** (Impact on men and women, potential link to carers below) No impact
4.3	**Race** (Consider different ethnic groups, nationalities, Roma Gypsies, Irish Travellers, language barriers, cultural differences). No impact
4.4	**Age** (Consider across age ranges, on old and younger people. This can include safeguarding, consent and child welfare). No impact
4.5	**Gender reassignment** (Consider impact on transgender and transsexual people. This can include issues such as privacy of data and harassment). No impact
4.6	**Sexual orientation** (This will include lesbian, gay and bi-sexual people as well as heterosexual people). No impact
4.7	**Religion or belief** (Consider impact on people with different religions, beliefs or no belief) No impact
4.8	**Marriage and Civil Partnership** No impact
4.9	**Pregnancy and maternity** (This can include impact on working arrangements, part-time working, infant caring responsibilities). No impact
4.10	**Carers** (This can include impact on part-time working, shift-patterns, general caring responsibilities, access to health services, 'by association' protection under equality legislation)**.** No impact
4.11	**Additional significant evidence (See Guidance Note)**

	Give details of any evidence on other groups experiencing disadvantage and barriers to access due to: • socio-economic status • location (e.g. living in areas of multiple deprivation) • resident status (migrants) • multiple discrimination • homelessness No impact
5 Action planning for improvement (See Guidance Note) Please give an outline of the key action points based on any gaps, challenges and opportunities you have identified. An Action Plan template is appended for specific action planning.	

Sign off
Name and signature of person who carried out this analysis Beverly Carter Head of IG, NHS South, Central and West Commissioning Support Unit
Date analysis completed 1 August 2013
Name and signature of responsible Director
Date analysis was approved by responsible Director

Appendix 2

Confidentiality agreement – NHS South, Central and West Commissioning Support Unit

Document name	NHS South, Central and West Commissioning Support Unit confidentiality agreement	
Date	1 April 2013	
Version	1	

Confidentiality agreement for third party suppliers

Who are third parties covered by this agreement?

Third party suppliers granted access to NHS South, Central and West CSU data and information in order to perform tasks as required by NHS South, Central and West CSU. They could include the following:

- Hardware and software maintenance and support staff (as defined in the scope) (for all of the document)
- Cleaning, catering, security guards and other outsourced support services (for general contractor clause and form on back page)

General contractor clause

(based on clause from Introduction to Data Protection in the NHS (E5127) and BS7799)

The Contractor undertakes:

- To treat as confidential all information which may be derived from or be obtained in the course of the contract or which may come into the possession of the contractor or an employee, servant or agent or sub-contractor of the contractor as a result or in connection with the contract; and

- To provide all necessary precautions to ensure that all such information is treated as confidential by the contractor, his staff, servants, agents or sub-contractors; and

- To ensure that he, his staff, servants, agents and sub-contractors are aware of the provisions of the Data Protection Act 1998 and BS7799 and that any personal information obtained from NHS South, Central and West CSU shall not be disclosed or used in any unlawful manner; and

- To indemnify NHS South, Central and West CSU against any loss arising under the Data Protection Act 1998 caused by any action, authorised or unauthorised, taken by himself, his staff, servants, agents or sub-contractors.

All staff, servants, agents and/or sub-contractors of the Contractor will be required to agree to and sign a confidentiality statement when they come to any of NHS South, Central and West CSU sites where they may see or have access to confidential personal and/or business information (see last page).

Supplier Code of Practice

The following Code of Practice applies where access is obtained to the NHS South, Central and West CSU, for the fulfilment of a required service.

The access referred to in paragraph 1 above may include:-

- Access to data/information on NHS South, Central and West CSU premises
- Access to data/information from a remote site
- Examination, testing and repair of media (e.g. fixed disc assemblies)
- Examination of software dumps
- Processing using CSU data/information

The Supplier must certify that his organisation is registered if appropriate under the Data Protection Act 1998 and legally entitled to undertake the work proposed.

The Supplier must undertake not to transfer any personal data/information out of the European Economic Area (EEA) unless such a transfer has been registered, approved by NHS South, Central and West CSU and complies with the Information Commissioners guidance on Safe Harbours.

The work shall be done only by authorised staff, servants, or agents of the contractor (except as provided in paragraph 12 below) who are aware of the requirements of the Data Protection Act 1998 and their personal responsibilities under the Act to maintain the security of NHS South, Central and West CSU personal data/information.

While the data/information is in the custody of the contractor it shall be kept in appropriately secure means.

Any data/information sent from one place to another by or for the contractor shall be carried out by secure means. These places should be within the suppliers own organisation or an approved sub-contractor.

Data/Information which can identify any patient/employee of NHS South, Central and West CSU must only be transferred electronically if previously agreed by NHS South, Central and West CSU. This is essential to ensure compliance with strict NHS controls surrounding the electronic transfer of identifiable personal data/information and hence compliance with the Data Protection Act 1998 and BS7799. This will also apply to any direct-dial access to a computer held database by the supplier or their agent.

The data/information must not be copied for any other purpose than that agreed by the supplier and NHS South, Central and West CSU.

Where personal data/information is recorded in any intelligible form, it shall either be returned to the Authority/Trust/Practice on completion of the work or disposed of by secure means and a certificate of secure disposal shall be issued to the Authority/Trust/Practice.

Where the contractor sub-contracts any work for the purposes in paragraph 1 above, the contractor shall require the sub-contractor to observe the standards set out in this agreement.

NHS South, Central and West CSU shall, wherever practical, arrange for the equipment or software to be maintained, repaired or tested using dummy data that does not include the disclosure of any personal data/information.

NHS South, Central and West CSU reserves the right to audit the supplier's contractual responsibilities or to have those audits carried out by a third party.

NHS South, Central and West CSU will expect an escalation process for problem resolving relating to any breaches of security and/or confidentiality of personal information by the suppliers employee and/or any agents and/or sub-contractors.

Any security breaches made by the supplier's staff, agents or sub-contractors will immediately be reported to the Caldicott Guardian of NHS South, Central and West CSU.

Certification form:

Name of supplier: _____

Address of supplier
prime contractor: _____

_____

_____

_____

Telephone number: _____

E-mail details: _____

On behalf of the above organisation I certify as follows:

The organisation is appropriately registered under the Data Protection Act 1998 and is legally entitled to undertake the work agreed in the contract agreed with the Authority/Trust/Practice

The organisation will abide by the requirements set out above for handling any of the Authority/Trust/Practice personal data/information disclosed to my organisation during the performance of such contracts

Signed: _____

Name of Individual: _____

Position in organisation: _____

Date: _____

Agreement outlining personal responsibility concerning security and confidentiality of information (relating to patients, staff (as defined in the scope) and the business of the organisation)

During the course of your time within the NHS South, Central and West CSU buildings, you may acquire or have access to confidential information which must not be disclosed to any other person unless in pursuit of your duties as detailed in the contract between NHS South, Central and West CSU and your employer. This condition applies during your time within NHS South, Central and West CSU and after that ceases.

Confidential information includes all information relating to the business of NHS South, Central and West CSU and its patients and staff.

The Data Protection Act 1998 regulates the use of all personal information and included electronic and paper records of identifiable individuals (patients and staff (as defined in the scope)). The Authority/Trust/Practice is registered in accordance with this legislation. If you are found to have used any information you have seen or heard whilst working within the Authority/Trust/Practice you and your employer may face legal action.

I understand that I am bound by a duty of confidentiality and agree to adhere to the conditions within the Contract between NHS South, Central and West CSU and my personal responsibilities to comply with the requirements of the Data Protection Act 1998.

NAME OF ORGANISATION:	
CONTRACT DETAILS:	
PRINT NAME:	
SIGNATURE:	
DATE:	

END OF DOCUMENT