NHS
Bristol, North Somerset and South Gloucestershire
Clinical Commissioning Group

Confidentiality and Security of Information Policy

Shaping better health

Please complete the table below: *To be added by corporate team once policy approved and before placing on website*	
Policy ref no:	11
Responsible Executive Director:	Sarah Truelove
Author and Job Title:	Information Governance Team
Date Approved:	October 2019
Approved by:	Governing Body
Date of next review:	October 2021

Policy Review Checklist

	Yes/ No/NA	Supporting information
Has an Equality Impact Assessment Screening been completed?	Yes	See Appendix 14.1
Has the review taken account of latest Guidance/Legislation?	Yes	
Has legal advice been sought?	No	Policy provided by SCW IG Team
Has HR been consulted?	Yes	Via Policy Review Group
Have training issues been addressed?	Yes	
Are there other HR related issues that need to be considered?	No	
Has the policy been reviewed by Staff Partnership Forum?	No	
Are there financial issues and have they been addressed?	No	
What engagement has there been with patients/members of the public in preparing this policy?	N/A	
Are there linked policies and procedures?	Yes	IG Policy, Subject Access Request, IG Policy, Records Management Policy
Has the lead Executive Director approved the policy?	Yes	
Which Committees have assured the policy?		Corporate Policy Group Governing Body
Has an implementation plan been provided?	Yes	
How will the policy be shared with		Policy will be available via the Hub

	Yes/ No/NA	Supporting information
Will an audit trail demonstrating receipt of policy by staff be required; how will this be done?	No	
Has a DPIA been considered in regards to this policy?	No	Not required, this policy provide general policy statements
Have Data Protection implications have been considered?		

Table of Contents

Confidentiality and Security of Information Policy

1 Introduction

The CCG has a legal obligation to comply with all appropriate legislation in respect of, Confidentiality, Data, Information and IT Security. It also has a duty to comply with guidance issued by NHS England, NHS Digital, the Information Commissioner's Office (ICO), Department of Health and other advisory groups to the NHS or professional bodies.

The ICO has the powers to impose fines or other penalties or corrective measures upon the organisation, and/or employees for non-compliance with relevant legislation and national guidance.

1.1 BNSSG CCG Values

This policy contributes to the values of the CCG by ensuring that the CCG does the right thing – it underpins individuals' right to privacy, ensures that confidential information is protected and facilitating the use and legitimate sharing of information enabling us to work better together.

2 Purpose and scope

This Confidentiality and Security of Information Policy details how the CCG will meet its legal obligations and NHS requirements concerning confidentiality, information security standards and will operate such procedures ensuring that confidential information sent to or from the organisation is handled in such a way as to minimise the risk of inappropriate access or disclosure. This policy applies to all staff and individuals working for or on behalf of the CCG.

For the purposes of this policy, where Personal or Special Categories of Data are described this will include data that is owed a duty of confidentiality under the Common Law.

3 Duties – legal framework for this policy

All staff have a legal duty of confidence to keep confidential data private and secure and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must not:

• Talk about confidential matters in public places or where they can be overheard.

• Leave any assets containing personal, commercially confidential or special categories of personal data lying around unattended, this includes telephone messages, computer printouts, faxes and other documents, or

• Leave a computer logged on to a system where information can be accessed or viewed by another person without authority to view that information

Staff must not use someone else's password to gain access to data. Action of this kind will be viewed as a serious breach of confidentiality under the Computer Misuse Act 1990 and in breach of CCG policies. This is a disciplinary offence and constitutes gross misconduct which may result in summary dismissal.

4 Responsibilities and Accountabilities

The Chief Executive Officer has overall responsibility for the Confidentiality and Security of Information Policy within the CCG. Where there is a significant concern regarding the ability of the CCG to evidence its obligations to handle information confidentially or a breach has occurred the matter will be brought to the attention of the CCG Executive Management Team. The IG Manager will work with the CCG to identify and report Information Governance risks and issues to the Information Governance Group (which includes Senior Information Risk Owner, Caldicott Guardian and Data Protection Officer).

The Information Manager (SCW) is contracted to provide Information Governance Services to the CCG, in particular they will provide advice and support on the implementation of this policy.

The Data Protection Officer is responsible for ensuring that that where an incident occurs and it is likely to result in a risk to the rights and freedoms of Data Subjects the Information Commissioner's Office is informed no later than 72 hours after the CCG becomes aware of the incident.

The day to day responsibilities for implementing this Policy will be devolved to all services and their Information Asset Owners and Administrators (IAOs and IAAs). In order that IAOs and IAAs can fulfil their roles, the SCW IG Team will support regular training and there will be regular IAO/IAA meetings to ensure they are aware of their responsibilities and the most effective way of ensuring adequate information security and confidentiality.

The CCG Information Governance Management Framework and Strategy details the hierarchical structure in place that underpins and ensures good governance processes are adhered to within the organisation.

5 Definitions/explanations of terms used – Security and Confidentiality

All information relating to Personal Confidential Data (PCD), as defined in the 'Confidentiality: NHS Code of Practice', personal, commercially confidential or special categories of personal data and any information that may be deemed confidential or 'sensitive', must be kept secure at all times. The CCG will ensure there are adequate policies and procedures in place to protect against unauthorised processing of information and against accidental loss, destruction and damage to this information.

Categories of Data

Personal Data (derived from the GDPR)	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
'Special Categories' of Personal Data (derived from the GDPR)	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: • The racial or ethnic origin of the data subject • Their political opinions • Their religious beliefs or other beliefs of a similar nature • Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 • Genetic data • Biometric data for the purpose of uniquely identifying a natural person • Their physical or mental health or condition • Their sexual life
Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).
Commercially	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be

confidential Information	damaging to SCW CSU or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

6 Safe Havens

A 'Safe Haven' is a term used to explain either a secure physical location or the agreed set of administration arrangements that are in place to ensure that personal data is communicated safely and securely. It is a safeguard for personal data, which enters or leaves the organisation whether this is by fax, post or other means.

All members of staff handling personal data, whether paper based or electronic, must adhere to relevant Safe Haven principles which should be documented and available to staff. For example within Finance there is a Controlled Environment for Finance which must follow agreed processes when handling patient data.

Where safe haven procedures should be in place

Safe haven procedures should be in place in any location where large amounts of personal or special categories of personal data is being received, held or communicated especially where the information is of a highly confidential nature.

Sending personal or special categories of personal data

Always consider whether it is necessary to share Personal or Special Categories of Personal data and if data minimisation can achieve the desired outcome. Within the NHS, confidential data should always be addressed to the appropriate safe haven within the recipient's organisation using the appropriate security classification for example:

OFFICIAL – SENSITIVE: COMMERCIAL

Definition - Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to CCG or a commercial partner if improperly accessed.

Or

OFFICIAL – SENSITIVE: PERSONAL

Definition - Personal information relating to an identifiable individual where inappropriate access could have damaging consequences

Some NHS organisations may still work to previous guidance; consequently any information received from an NHS organisation may be marked as NHS Confidential which should then be treated as OFFICIAL – SENSITIVE depending on its type.

For specific guidance and procedures in respect of telephony enquiries, e-mails, faxes and post, please refer to the IG guidance.

7 Processes and Requirements

Database Management

All databases should form part of an Information Asset Register (IAR). A list of the organisations IAR's will be maintained by SCW IG Team but remain the responsibility of the individual team Information Asset Owner's (IAO's) in the CCG.

For the purposes of this policy the term "Database" refers to a structured collection of records or data held electronically which contains personal or special categories of personal data, which has been provided in confidence or commercially confidential data. In the event that further guidance is needed in respect to what constitutes a database please contact the SCW IG Team.

Back Ups

SCW IT Services Teams are responsible for ensuring that appropriate back up procedures are available and implemented.

Disclosure of Information & Information Flows

It is important that information that identifies individuals (such as the general public, patients and/or staff) should only be shared on a strict need to know basis and with the appropriate authorisation. Strict controls governing the disclosure of identifiable information is a requirement of the Caldicott recommendations.

All disclosures or flows of data, either electronically or in hard copy, which contain personal, special categories of personal data, or commercially confidential information and indeed any information that may be deemed confidential or 'sensitive' must be included in the relevant IAR and Data Flow Mapping (DFM) tool.

If any personal, commercially confidential or special categories of personal data need to be shared electronically via removable media devices (such as encrypted disc, encrypted USB memory stick etc.) or manually (for hard copy records) via courier or postal service, a Data Protection Impact Assessment (DPIA) should be considered and carried out where the security and confidentiality of this information is potentially at risk. For further guidance or advice please contact the SCW IG Team.

Contracts between the CCG and third parties with whom information is shared must include appropriate Data Protection and Confidentiality clauses.

The CCG is a 'Controller' either solely or jointly, as defined in the General Data Protection Regulation (GDPR), and uses 'Processors' or 'sub Processors'. All of whom are obliged to meet the requirements of the Data Protection Legislation and must be correctly identified in contracts and agreements with standard checks of evidence of compliance undertaken prior to contract terms being signed. Processors must only act in accordance with directions from the identified Controller.

Where the CCG commissions providers to provide clinical services the relationship is different, the provider will normally be a Data Controller in their own right.

Disclosure of Information outside the European Economic Area (EEA)

No personal, commercially confidential or special categories of personal data should be disclosed or transferred outside of the European Economic Area (EEA) to a country or territory which does not ensure an adequate level of protection unless certain exemptions apply or adequate protective measures are taken which are in accordance with those set out and stated in the Data Protection Legislation.

In the event that there is a need to process information outside of the EEA, the Data Protection Officer must be consulted prior to any agreement to transfer or process the information. A statutory Data Protection Impact Assessment (DPIA) must be completed, reviewed and approved when considering any new processing of information in these circumstances.

The Legal Basis for sharing personal, commercially confidential or special categories of personal data

To ensure that data is shared appropriately, care must be taken to check that a clear basis in law is established that permits or obligates the sharing. The completion of a DPIA is a statutory requirement when considering new processing including the sharing of Special Categories of personal data as defined in the GDPR.

It is important to consider how much data is required and ensure that the minimal amount necessary is disclosed.

Data can normally be disclosed when effectively anonymised/pseudonymised in line with legislative requirements and the ICO Anonymisation Code of Practice, unless subject to other restrictions e.g. NHS Digital contracts.

When the information is required by law or under a court order in situations such as the detection and prevention of serious crime, staff should discuss the matter with the Information Governance Manager in the first instance with reference to the Data Protection Officer and Caldicott Guardian for further advice, support and where necessary to approve the disclosure.

Data can be disclosed in identifiable form, with the individual's explicit consent or the appropriate lawful basis under the GDPR or with support from NHS England who will apply for the necessary approval from the appropriate authority for example, the Confidentiality Advisory Group (CAG).

In potential safeguarding situations where it is decided that information should be shared according to the duties placed on the organisation to protect vulnerable people, staff should contact their line manager and if necessary, discuss with the Data Protection Officer, who will provide advice and guidance and in cases where a decision to share is not clear. Where necessary it may be prudent to inform and obtain approval of the Caldicott Guardian for the disclosure.

When necessary and agreed as part of the DPIA process, a Data Sharing, Data Processing or Transfer of Service Agreement must be completed before any data is transferred. The various agreements will set out any conditions for use and identify the secure method of transfer. For further information on Data Sharing Agreements contact the SCW IG Team.

Care must be taken when transferring data to ensure that the method used is encrypted where necessary and is always secure. Staff must ensure that appropriate standards and safeguards are in place in respect of telephony enquiries, e-mails, faxes and post.

It is policy that emails containing any personal, commercially confidential or special categories of personal data should be sent using an NHS.net account. Therefore, staff emailing from @nhs.net accounts to another @nhs.net account, can be confident that the content of the message is encrypted and secure.

In circumstances where the receiving organisation does not hold a NHS.net account, the Encryption Guide for NHSmail must be followed to ensure all personal, commercially confidential or special categories of personal data sent outside of NHSmail is protected.

The service dictates you must use [secure] in square brackets in the subject line of your email. An encrypted email sent from an NHSmail address (ending @nhs.net) will contain a link to access the encrypted message.

Staff must ensure they use the NHSmail platform in accordance to the published guidance, policies and procedures to ensure appropriate and secure usage NHS mail guidance.

Care must be taken to ensure confidential information is not entered in the subject header when sending an email. Please seek advice from SCW IG Team if required.

If information is required to be sent to a member of the public, using their non-secure email address, it is the responsibility of the member of staff to ensure that the member of public is provided with a clear explanation of the risks of using unsecure email addresses and records of this conversation should be kept.

There are Acts of Parliament, listed below (not exhaustive), which govern the disclosure of personal and special categories of personal data. Some of these Acts make it a legal requirement to disclose and others state that information cannot be disclosed.

- Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1985
- Education Act 1944 (for immunisations and vaccinations to NHS Public Health England from schools)
- Births and Deaths Act 1984
- Police and Criminal Evidence Act 1984
- Human Fertilisation and Embryology (Disclosure of Information) Act 1992

- Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992
- Abortion Act 1967
- The Adoption Act 1976
- Children Act 2004

In the event that a request for disclosure is made referencing any of these Acts appropriate advice and support should be sought and the Data Protection Officer to advise.

Mobile and remote working

There will be times when staff may need to work from another location or work remotely. This means that these staff may need to carry organisational data and assets with them which could be or contain personal, commercially confidential or special categories of personal data e.g. on an encrypted laptop, encrypted USB stick or as paper documents.

When taking paper documents that contain confidential information outside of the normal office environment, approval should be obtained from your line manager and a risk assessment completed where there is the potential for data loss to occur. In completing a risk assessment the following should be considered:

- What information is being transported outside the normal office environment? Does it relate to individuals? If so how many?
- Is it absolutely necessary – can information be reduced or anonymised in any way?
- What protections are there in place? E.g are the papers secured in a sealed envelope?
- What would the impact be if the papers where lost or made available to unauthorised individuals?

When working away from CCG locations, staff must ensure that their working practices comply with CCG policies and procedures. Any removable media must be encrypted as per the NHS Encryption Guidance Standards.

Staff must not leave personal, commercially confidential or special categories of personal data unattended at any time and ensure that it is kept in a secure lockable place when working remotely.

Staff must minimise the amount of personal, commercially confidential or special categories of personal data that is taken away from CCG premises.

When in transit staff must ensure that any personal, commercially confidential or special categories of personal data is transported in a secure manner, is kept out of sight whilst being transported (i.e. the boot of a car) and removed to a more secure location on arrival at their destination. Do not leave equipment or assets in a car.

Staff are responsible for ensuring that any data or assets taken home are kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have access to the data.

Staff must not forward any personal, commercially confidential or special categories of personal data via email to their home email account or store the data on a privately owned computer, storage device or other technology such as a cloud storage solution that is not provided by the CCG.

8 Confidentiality Audits

Good practice requires that all organisations that handle personal, commercially confidential or special categories of personal data put in place processes to highlight actual or potential breaches of security or confidentiality in their systems, and also procedures to evaluate the effectiveness of controls within these systems. This function will be co-ordinated by SCW Information Governance Team through a programme of audits. Regular audit for relevant systems and processes will be scheduled. Confidentiality Audits will be undertaken at least annually.

9 Contracts of Employment

Staff contracts of employment are produced and supported by SCW Human Resources (HR) department. All contracts of employment include a clause on adherence to the data protection legislation and the common law duty of confidentiality. Agency and non-contract staff working on behalf of the CCG are subject to the same rules which will be enforced and recorded through the use of a confidentiality agreement. Template agreements are included in Appendix 17.3.

All employees will be made aware of their responsibilities through their Statement of Terms and Conditions, their information governance training, staff induction and all relevant policies, procedures and guidance.

10 Disciplinary

A breach of the Data Protection Legislation requirements could result in a member of staff facing disciplinary action. A copy of the Disciplinary Procedure is available from the HR Department.

11 Abuse of Privilege

It is strictly forbidden for employees to knowingly browse, search for or look at any data relating to themselves, their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and the Data Protection Legislation.

Members of staff who would like exercise their ‘right of access’, as defined in the GDPR, for the personal data held by the organisation can do so by submitting a subject access request.

12 Training requirements

Information Asset Owner and Information Asset Administrators

The SCW IG Team provides awareness of confidentiality and security issues for all staff covering:

- How to provide awareness to teams regarding their personal responsibilities, such as locking doors and avoiding gossip in open areas
- Confidentiality of personal and commercial data
- Relevant NHS Policies and Procedures e.g. Record Management Lifecycle Protocol
- Compliance with the Data Protection Legislation and Caldicott Guardian principles
- Individual rights under the GDPR covering but not limited to the rights of access, rectification, erasure and data portability
- General good practice guidelines covering security and confidentiality
- A general overview of all Information Governance requirements
- A brief overview of the Data Protection Legislation.
- Data Protection Impact Assessments
- The Information Asset Owner work programme – Information Asset Registers and Data Flow Mapping etc.

All Staff

All new starters to the CCG inclusive of temporary, bank staff and contractors must undertake Data Security and Awareness training via the ConsultOD portal, to evidence compliance with the Data Protection Legislation and the DSP Toolkit assertions as part of the induction process. Extra training will be given to those dealing with formal requests for access to personal information. A register will be maintained of all staff who have completed the online training and those who have attended face to face training sessions where these are offered.

Annual Data Security and Awareness training should be undertaken by all staff via the ConsultOD portal.

All staff will be made aware of what could be classed as an information security incident or breach of confidentiality and the process to follow and the location of the forms to complete. This ensures incidents can be identified, reported, monitored and investigated.

13 Equality Impact Assessment – DPIA

An Equality Impact Analysis (EIA) screening has been completed. A copy of the EIA is attached at Appendix 14.1.

14 Implementation and Monitoring Compliance and Effectiveness

This Policy will be reviewed every two years or more frequently if appropriate, to take into account changes to legislation that may occur, and/or guidance from NHS

England, NHS Digital and the Information Commissioner or any relevant case law. The next full review will be undertaken in September 2021, unless changes in law or practice require review.

This policy will be monitored by the SCW IG Team to ensure any legislative changes that occur before the review date are incorporated.

15 Countering Fraud

The CCG is committed to reducing fraud in the NHS to a minimum, keeping it at that level and putting funds stolen through fraud back into patient care. Therefore, we have given consideration to fraud and corruption that may occur in this area and our responses to these acts during the development of this policy document.

16 References, acknowledgements and associated documents

For the purpose of this Policy other relevant legislation and appropriate guidance may be referenced. The legislation listed below also refers to issues of security of personal confidential data.

- General Data Protection Regulations 2016
- Data Protection Act 2018
- Access to Health Records 1990
- Access to Medical Reports Act 1988
- Human Rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Crime and Disorder Act 1998
- Computer Misuse Act 1990
- Criminal Justice and Immigration Act 2008
- Health and Social Care Act 2012
- Health and Social Care (Safety and Quality) Act 2015
- The Privacy and Electronic Communications (EC Directive) Regulations 2003

The following are the main publications referring to security and or confidentiality of personal confidential data:

- Confidentiality: NHS Code of Practice
- CQC Code of Practice on Confidential Personal Information
- NHS Digital: A Guide to Confidentiality in Health and Social Care
- NHS England Confidentiality Policy
- Records Management Code of Practice for Health and Social Care Information Security: NHS Code of Practice
- Employee Code of Practice (Information Commissioner)
- Caldicott Report 1997 and 2013
- Caldicott 3- Review of Data Security, Consent and Opt-Outs

This Policy should be read in conjunction with other Information Governance (IG) Policies including:

Information Governance Policy

Records Management Policy

Individual Rights Policy

Incident Reporting Policy

17 Appendices

17.1 Equality Impact Assessment

Equality Impact Assessment Screening		
Query	**Response**	
What is the aim of the document?	The Confidentiality and Security of Information Policy details how the CCG will meet its legal obligations and NHS requirements concerning confidentiality, information security standards and operates such procedures ensuring that confidential information sent to or from the CCG is handled in such a way as to minimise the risk of inappropriate access or disclosure. For the purposes of this policy, where Personal or Special Categories of Data are described this will include data that is owed a duty of confidentiality under the Common Law.	
Who is the target audience of the document (which staff groups)?	All staff	
Who is it likely to impact on and how?	Staff	X
	Patients	X
	Visitors	X
	Carers	X
	Other – governors, volunteers etc	X
Does the document affect one group more or less favourably than another based on the 'protected characteristics' in the Equality Act 2010:	Age (younger and older people)	
	Disability (includes physical and sensory impairments, learning disabilities, mental health)	
	Gender (men or women)	
	Pregnancy and maternity	
	Race (includes ethnicity as well as gypsy travelers)	
	Sexual Orientation (lesbian, gay and bisexual people)	
	Transgender people	
	Groups at risk of stigma or social exclusion (e.g. offenders, homeless people)	
	Human Rights (particularly rights to privacy, dignity, liberty and non-degrading treatment)	

17.2 Implementation Plan

Target Group	Implementation or Training objective	Method	Lead	Target start date	Target End date	Resources Required
Staff	To have policy available to all staff	To be published on the Hub	Comms/IG	01/10/2019	31/10/2019	Comms team
Staff	To ensure all staff are aware of the policy	To include summary of highlights in The Voice	Comms/IG	01/10/2019	31/10/2019	Comms team

17.3 Confidentiality Agreement templates

These templates to be used where the standard NHS contract is not is use, advice can be obtained from the IG Manager

Confidentiality agreement for third party suppliers

The following confidentiality agreement clauses can be used for agreements with relevant third parties.

Who are third parties covered by this agreement?

Third party suppliers granted access to CCG data and information in order to perform tasks as required by the CCG. This could include the following:

- Hardware and software maintenance and support staff (for all of the document)
- Organisations or staff employed under contract on an interim basis to process CCG information
- Cleaning, catering, security guards and other outsourced support services (for general contractor clause and form on back page)
- Auditors

General contractor clause

The Contractor undertakes:

- To treat as confidential all data 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 data is treated as confidential by the contractor, his employees, servants, agents or sub-contractors; and
- To ensure that they, their employees, servants, agents and sub-contractors are aware of the provisions of Data Protection Legislation and ISO/IEC 27001 and that any personal and special categories of personal data (held confidentially or otherwise) and commercially confidential information obtained from the CCG shall not be disclosed or used in any unlawful manner; and
- To indemnify the CCG against any loss arising under the Data Protection Legislation caused by any action, authorised or unauthorised, taken by himself, his employees, servants, agents or sub-contractors.

All employees, 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 the CCG sites where they may see or have access to personal, commercially confidential or special categories of personal data.

Supplier Code of Practice

The following Code of Practice applies where access is obtained to CCG information for the fulfilment of a required service.

The access referred to in paragraph above may include:-

- Access to data/information on CCG 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 CCG data/information

The Supplier must certify that their organisation is registered as appropriate with the Information Commissioners Office under the Data Protection Legislation and is competent to undertake the work proposed.

The Supplier must undertake not to transfer any personal, commercially confidential or special categories of personal data out of the European Economic Area (EEA) unless such a transfer has been agreed, registered and approved by the CCG and complies with the Information Commissioners guidance.

The work shall be done only by authorised employees, servants, or agents of the contractor who are aware of the requirements of the Data Protection Legislation and of their personal responsibilities under the Legislation to maintain the security of CCG data.

The data in the custody of the contractor shall be kept in an appropriately secure format and any transfer of such data, from one place to another, must be carried out by secure encrypted means. These places should be within the suppliers own organisation or an approved sub-contractor.

Data must only be transferred electronically if either explicit consent has been given or another appropriate legal basis to process has been established; the data is encrypted and previously agreed by the organisation. This is essential to ensure compliance with strict NHS controls surrounding the transfer of personal or special categories of personal data and compliance with the Data Protection Legislation. These rules also apply to any direct-dial access to a computer held database by the supplier or their agent.

The data must not be copied for any other purpose than that agreed by the supplier and the CCG.

Where personal, commercially confidential or special categories of personal data is recorded in any intelligible form, it shall either be returned to the CCG on completion of the work or disposed of by secure means and a certificate of secure disposal shall be issued by the organisation to the CCG. A system exit strategy must be put in place.

Where the contractor sub-contracts any work for the purposes of the contract delivery, the contractor shall require the sub-contractor to observe the standards set out in this agreement and must be authorised by the CCG.

The CCG 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, commercially confidential or special categories of personal data.

The CCG reserves the right to audit the supplier's contractual responsibilities or to have those audits carried out by a third party.

The CCG will expect an escalation process for problem resolution relating to any breaches of security and/or confidentiality of data by the suppliers employee and/or any agents and/or sub-contractors.

Any security breaches made by the supplier's employees, agents or sub-contractors will immediately be reported to the designated lead and will be recorded and escalated to the Data Protection Officer, Caldicott Guardian and Senior Information Risk Owner.

Certification form

Name of Supplier _____

Address of Supplier (prime contractor) _____

_____

_____

_____

_____

Telephone number _____

Email details _____

On behalf of the above organisation I certify as follows:

The organisation is appropriately registered with the Information Commissioners Office and is competent to undertake the work agreed in the contract agreed with the CCG. The organisation will abide by the requirements set out above for handling any personal, commercially confidential or special categories of personal data disclosed to my organisation during the performance of such contracts

Signature _____

Name of Individual _____

Position in Organisation _____

Date _____

Individual Agreement

This agreement outlines your personal responsibility concerning the security and confidentiality of CCG information (this includes personal and special categories of personal data (deemed confidential or otherwise) or Commercial/commercially confidential information.

During the course of your time within CCG buildings or working on behalf of the CCG, you may acquire or have access to information which must not be disclosed to any other person unless in pursuit of your duties as detailed in the contract between the CCG and you/your employer. This condition applies during your time within the CCG and endures after that ceases.

As part of the contract you may create or process documents and other information that will remain the property of the CCG at all times. Any use of any template or document originally created for CCG purposes will not be permitted after the contract ends unless this is agreed prior to this date or authorised post contract end date. This should be discussed with the person responsible for overseeing the activities you have undertaken whilst contracted to the CCG.

Confidential information includes all information relating to the business of the CCG and its patients and employees. The Data Protection Legislation regulates the use of all personal data and includes electronic and paper records of identifiable individuals (patients and staff). If you are found to have used any information you have seen, heard or been privy to whilst working within the CCG for any other purpose than that which it was shared with you both 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 the organisations and my personal responsibilities to comply with the requirements of the Data Protection Legislation.

Name of Organisation: _____

Contract Details: _____

Print Name: _____

Signature: _____

Date: _____