NHS
Buckinghamshire
Clinical Commissioning Group

Confidentiality and Safe Haven Policy

Buckinghamshire CCG

Version 2.2 - **May 2021**

Version Number: 2.2	Issue/approval date: May 2021
Status: Final	Next review date: May 2022

NHS
Buckinghamshire
Clinical Commissioning Group

Document Control

Document Name	Version	Status	Author
Confidentiality and Safe Haven Policy	2.2	Final	Information Governance Services
Document objectives:	This policy describes BCCG's responsibilities under the Data Protection Legislation and ensures all employees abide by the common law duty of confidence and Safe Haven Framework to protect personal confidential data and the Safe Haven framework ensuring all staff are informed of their operational and legal responsibilities.		
Target audience:	All staff		
Committee/Group Consulted*:*	BCCG Information Governance Steering Group		
Monitoring arrangements and indicators:	This policy will be monitored by the Information Governance Team to ensure any legislative changes that occur before the review date are incorporated.		
Training/resource implications:	All Staff - Dissemination will take place using the Staff bulletin and will be displayed on the CCG's intranet IG team pages		
Approved and ratified by:	BCCG Information Governance Steering Group. Audit Committee.	Date: May 2021 Date: July 2021	
Equality Impact Assessment:	Yes	Date: 08-06-18	
Date issued:	May 2021		
Review date:	May 2022		
Author:	Information Governance Team		
Lead Director:	CCG Caldicott Guardian (Dr. Karen West)		

Version Control

Change Record

Date	Author	Version	Page	Reason for Change
14-05-18	SCW CSU	V.1.0	All	Review due to changes in Data Protection Legislation and amalgamation of the Safe Haven Policy
Jan 2019	BCCG	V.2.0	All	Review due to changes in Data Protection Legislation and amalgamation of the Safe Haven Policy for the CCG
March 2019	BCCG	V2.1	All	Amendments to job titles to reflect local arrangements
May 2021	BCCG	V2.2	All	Change of GDPR to UK GDPR as a result of UK-EU withdrawal agreement. Added the 8th Caldicott Guardian Principle in the policy.

Contents

Document Control 2

1. **Introduction** 5
2. **Scope and Definitions** 5
3. **Processes/Requirements** 5
4. **Staff Responsibilities** 11
5. **Confidentiality Audits** 12
6. **Roles and Responsibilities** 12
7. **Training** 12
8. **Contracts of Employment** 13
9. **Disciplinary** 14
10. **Abuse of Privilege** 14
11. **Public sector equality duty- equality impact assessment** 14
12. **Monitoring compliance and effectiveness** 14
13. **Review** 14
14. **References and associated documents** 14

Appendix A: Confidentiality Agreement template – third parties 16

Appendix B: Confidentiality Agreement template – substantive staff 21

Appendix C: Equality Impact Analysis 216

1. Introduction

The NHS Buckinghamshire 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, NHSX, 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 CCG, and/or employees for non-compliance with relevant legislation and national guidance.

2. Scope and Definitions

This Confidentiality and Safe Haven 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.

Safe Haven

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 within an organisation to ensure that patient or staff 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 the Safe Haven principles. The requirements within the Policy are primarily based upon the Data Protection Legislation covering security and confidentiality of personal data.

3. Processes/Requirements

Security & 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 indeed 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 confidential Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to BCCG or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

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 release 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 safe haven of the recipient's organisation using the appropriate security classification on their documentation as follows:

All information used by the BCCG by definition 'OFFICIAL.'

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

NHS Confidential

In the interim, some NHS organisations may still work to existing IG 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.

This BCCG guidance maps to current NHSE Records Management guidance.

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

Database Management

SCW Information Governance (IG) Team advise that 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 and/or staff) should only be disclosed on a strict need to know basis with the appropriate relevant authorisation approved. Strict controls governing the disclosure of identifiable information is also 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.

Some disclosures and flows of data may occur because there is a statutory duty on the CCG to disclose e.g. a Court Order or because other legislation requires disclosure (staff tax returns or the pension's agency).

If any personal, commercially confidential or special categories of personal data need to be transported 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 must include appropriate Data Protection and Confidentiality clauses.

The CCG is a 'Controller' either solely or jointly, as defined in the UK General Data Protection Regulation (UK 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.

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 and appropriate authorisation to do so is in place. 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 be disclosed when effectively anonymised/pseudonymised.in line with legislative requirements and the ICO Anonymisation Code of Practice.

When the information is required by law or under a court order in situations such as the detection and prevention of serious crime, staff must discuss the matter with the Data Protection Officer, who will provide advice and guidance and inform and obtain approval of the Caldicott Guardian for the disclosure.

Data can be disclosed in identifiable form, with the individual's explicit consent or the appropriate legal basis under the UK GDPR or 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 various duties placed on NHS organisations 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. See the IG Staff Handbook for guidance on the safe transfer of personal, commercially confidential or special categories of personal data.

It is policy that emails containing any personal, commercially confidential or special categories of personal data should be sent using an NHS.net account or any other e-mail domain accredited to NHS Digital's DCB1596 standard. Therefore, staff emailing from

@nhs.net accounts to another @nhs.net account or to another e-mail account accredited to DCB1596 standard, 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 or any other e-mail account accredited to DCB1596 standard, 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 the NHSmail platform operates 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 consent should be obtained and recorded.

There are additional Acts of Parliament, listed below but not exhaustive, which governs the disclosure of personal and special categories of personal data. Some of these Acts make it a legal requirement to disclose and others that 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 the Data Protection Officer must be notified prior to any information being released.

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 CCG 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.

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 lockable container and secure manner, is kept out of sight whilst being transported (i.e. I 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 any 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 SCW.

4. Staff Responsibilities

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 SCW IT policies. This is a disciplinary offence and constitutes gross misconduct which may result in summary dismissal.

5. 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 IT Services Team through a programme of audits. Regular audit for relevant systems should be scheduled. Confidentiality Audits will be undertaken at least annually by Data Custodians.

6. Roles and Responsibilities

The Chief Officer has overall responsibility for the Confidentiality and Safe Haven 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 Committee. The Information Governance Manager is responsible for reporting Information Governance risks and issues to the Information Governance Steering Group.

The Data Protection Officer will ensure that where an incident is likely to result in a risk to the rights and freedoms of Data Subjects the ICO is informed no later than 72 hours after the organisation becomes aware of the incident.

The day to day responsibilities for implementing this Policy will be devolved to the IAO's and DC's. In order that IAOs and DC's fulfil their roles, the SCW IG Team will support regular training 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.

7. Training

Information Asset Owner, Data Custodians or Information Asset Administrators

The SCW IG Team can support awareness of confidentiality and security issues for all staff. Detailed training will cover:

- 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
- Registration of automated databases
- Individual rights under the UK 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
- How to inform staff about the relevant policies and procedures and also how to provide good practice guidance.
- A brief overview of the Data Protection Legislation.
- Data Protection Impact Assessments
- The Data Custodian work programme

All Staff

All new starters to the CCG inclusive of temporary, bank staff and contractors must undertake Information Governance induction training via the E-Learning for Health (e-LfH) IG Training tool, to evidence compliance with the Data Protection Legislation and the Data Security and Awareness DSP Toolkit assertions as part of the induction process. Extra training will be given to those dealing with requests for 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 IG training should be undertaken by all staff via the e-LfH Data Security Awareness modules as made available through the ConsultOD portal or face to face training.
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.

Please see IG Services Incident Management and Reporting Procedure for further guidance on this area.

8. 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 NHS are subject to the same rules which will be enforced and recorded through the use of a confidentiality agreement.

All employees will be made aware of their responsibilities in connection with the relevant legislations mentioned in this Policy through their Statement of Terms and Conditions, their information governance training, staff induction, the IG staff handbook and all relevant policies, procedures and guidance.

9. 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.

10. 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 UK GDPR, for the personal data held by the CCG or SCW can do so by submitting a subject access request.

11. Public sector equality duty- equality impact assessment

An Equality Impact Analysis (EIA) has been completed. No adverse impact or other significant issues were found. A copy of the EIA is attached at Appendix B.

12. Monitoring compliance and effectiveness

This policy will be monitored by the SCW IG Team to ensure any legislative changes that occur before the review date are incorporated. Please refer to Individual Rights policy for guidance on how to handle a 'Right to Access' Subject Access Request or Access to Records requests.

13. Review

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 May 2022.

14. References 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:

- UK General Data Protection Regulations 2018
- UK 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 the Information Governance (IG) Policy and Framework, the Records Management Policy and the Information Governance Staff Handbook.

Appendix A: Confidentiality Agreement template

Confidentiality Agreement

Document name	Confidentiality Agreement – third party suppliers/contractors
Date:	April 2019
Author	Information Governance Team, NHS South, Central and West CSU Russell Carpenter, CCG Head of Governance/Board Secretary
Version	8

*(**Instructions**: This statement is to be read and signed in DUPLICATE by all personnel when they first start with the Clinical Commissioning Group (CCG). There is a separate version for permanent staff on NHS contracts. One copy is to be retained by the signatory and one copy to be held by the CCG).*

Confidentiality agreement for third party suppliers

Who are third parties covered by this agreement?
Third party suppliers granted access to BCCG data and information in order to perform tasks as required by the CCG. They 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, their 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 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 an employee, servant, agent or sub-contractor working for the CCG in in agency, interim or otherwise temporary capacity

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 1 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 which can identify an individual of the CCG must only be transferred electronically if explicit consent has been given or 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, 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: _____

Appendix B: Confidentiality Agreement – substantive staff

Confidentiality Agreement – substantive staff

*(**Instructions**: This statement is to be read and signed in DUPLICATE by all personnel when they first start with the Clinical Commissioning Group (CCG). There is a separate version for agency/interims/third party staff. One copy is to be retained by the signatory and one copy to be held by the CCG).*

Introduction

All employees including agency staff, interims, contractors and volunteers are responsible for maintaining confidentiality. This duty of confidentiality forms part of your employment/engagement contract. Breach of information gained in the course of duty may lead to disciplinary action that could result in dismissal. You should also be aware that regardless of any disciplinary action taken, a breach of confidence could also result in civil action for damages.

In the course of your duties you may have access to confidential information. This will include information about patients, clients, staff records, details of contract prices and terms and other business sensitive data.

Gaining access or attempting to gain access to information that you do not need to see to carry out your work is a breach of confidentiality, as is passing information on to someone who is not authorised to receive it.

You must not, whether during or after your employment/engagement with the organisation, unless expressly authorised by the Accountable Officer, make any disclosure to any unauthorised person or use any confidential information relating to the business affairs of the Organisation. This includes any detail about the CCG clients and employees, actual, potential or past and all details relating to information on any of the CCG databases.

Basic Principles

Generally personal information given for one purpose must not be used for another purpose without the consent of the person concerned because that use may breach confidentiality.

Everyone has a legal right to know what information is being collected about them and why, and the purposes for sharing that information.

For patients, consent cannot be implied for purposes other than healthcare. Non-healthcare purposes could include disclosure to the police, to government departments other than the Department of Health, to the courts, etc. In most cases, patients should be asked for their

explicit consent before information is shared for non-healthcare purposes. Seek advice if you are not sure whether specific consent is required.

Every individual has an obligation to protect confidentiality and a duty to verify the authorisation of another person to ensure information is only passed on to those who have a right to see it and to follow the rules and guidance available to them.

The rules are there to protect both patient and staff but they should not be applied so rigidly that they are impractical to follow or detrimental to the care of the individual concerned. If in doubt seek advice.

You are responsible for your decision to pass on information. If you are unsure whether or not to disclose information, consult your line manager and/or if necessary obtain advice from the Head of Corporate Governance, the Caldicott Guardian, Information Governance Officer or information security team.

Relevant Legislation
Individuals are required to ensure that confidential information is safeguarded and is kept securely in accordance with all relevant legislation. This includes:

UK Data Protection Act 2018
Use of personal data should be:

1. Fair and lawful
2. Used only for specified and lawful purposes
3. Adequate, relevant and not excessive
4. Accurate and kept up to date
5. Not kept for longer than necessary
6. Processed in accordance with data subject rights
7. Kept secure and protected against accidental disclosure, loss or damage
8. Not transferred outside the EEA

The Act regulates the use of all information relating to any living identifiable individual that the Organisation may hold, regardless of the media in which it is held. This information may be as basic as name and address. Unauthorised disclosure of any of this information may be deemed a criminal offence. If you are found to have permitted the unauthorised disclosure of any such information, you and the Organisation may face legal action.

Human Rights Act 1998
Article 8: Everyone has the right to respect for their private and family life, home and correspondence.

It is unlawful for a public authority to act in a way that is incompatible with a convention right.

Common Law Duty of Confidence

Information obtained for one purpose should not be used for another purpose without the express or implied authorisation (consent) of the provider of that information.

Caldicott Principles

The general principles underlying the use and sharing of personal information are:

- Justify the purpose for using confidential information
- Only use it when absolutely necessary
- Use the minimum identifiable information required for that purpose
- Access should be on a strict 'need to know' basis
- Everyone must understand their responsibilities to protect information
- Everyone must understand and comply with the law.
- Inform patients and service users about how their confidential information is used.

Your Duty of Care

You are responsible for protecting the physical security of confidential information from accidental loss, damage, destruction, unauthorised access or accidental disclosure. For example:

Physical Security

- You must return to the CCG upon request (and in any event upon the termination of your employment/engagement), all documents and tangible items which belong to the Organisation or which contain or refer to any confidential information and which are in your possession or under your control
- You must not remove or copy any documents, regardless of their format i.e. electronic or hard copy, or tangible items including software which belong to the CCG or which contain any confidential information from the Organisation's premises at any time without proper advanced authorisation
- Do not leave confidential information lying around unattended or place paper containing confidential information in the bin. It must be shredded or put in a 'confidential waste' container
- You should always wear your identification badge when on CCG premises. Challenge unknown persons on the premises
- Lock away any confidential information and lock offices when unoccupied
- Do not remove confidential data (held manually or electronically) from CCG sites without the express permission of your Manager/Head of Service/Director. If this is required as part of your job then you are responsible for following the guidelines for storing and transporting confidential information as set out in the Information Security Policy
- Be especially careful with the security of portable computers, i.e. hand held devices and laptops and follow the principles set out in the Information Security Policy
- Take care when giving personal information over the phone – have you identified the person? Do they have a right to know? Can anybody else hear the conversation?
- Be careful when putting a telephone call on hold – what information might they hear?

- Don't leave personal information on answer phones
- Envelopes containing confidential information **must** be securely sealed, labelled **'confidential'** and clearly addressed to a known contact. Medical records or other sensitive information should be sent externally by Special Delivery or by approved courier. Please refer to the Information Security Policy for more information

Computer and Electronic Security

- Keep your PC screen out of sight of others if personal information is showing and log out or lock your computer keyboard if you move away from your desk
- Never tell anyone your password or share passwords. Change your password regularly
- Do not email or fax patient identifiable information unless approved safeguards are used or there are exceptional circumstances. Consult your line manager if personal or confidential information has to be sent in this way and refer to the Information Security Policy for instructions.
- Ensure you store all information on a backed-up shared drive and **not** on the hard drive/desktop of your computer. Do not keep or process CCG confidential/identifiable data on your home PC
- Under no circumstances should you put software on a CCG PC without permission of the head of the IT department
- Under no circumstances should you connect non-NHS supplied equipment to the NHS network or computers – for example personal lap tops, IPhones, IPods.
- The only memory sticks which are permitted for use are those provided by the IT procurement department, which are fully encrypted and meet NHS security requirements.

Intellectual Property

If at any time as a part of your work with the CCG you develop, discover or participate in the development or discovery of any Intellectual Property, the full details of the Intellectual Property shall be immediately communicated to the organisation and shall be the absolute property of the organisation. At the request and expense of the organisation you agree to provide all such information, data, drawings and assistance as may be required to exploit the Intellectual Property to best advantage and to execute all documents and do all things which may be necessary or desirable for obtaining a patent or other protection in such parts of the world as specified by the organisation and for vesting the same in the organisation or as it may direct. In addition, if as part of your work, you are exposed to the detail of any existing intellectual property of the CCG, you undertake to respect the commerciality of that property and not to utilise that knowledge in any way for your personal gain.

All rights and obligations shall continue in force after termination of your appointment in respect of Intellectual Property developed/discovered during the period of your work with the CCG.

General

- Report any security risks/incidents
- Always protect your data
- Ensure that you have accurate and correct information
- Don't keep information longer than necessary – refer to your line manager
- Do not discuss confidential information with friends or family outside of the CCG or with colleagues in public places
- Read all related policies and guidance on confidentiality and information security
- Do not set up any databases or new information flows for personal data without discussing it with the Head of Corporate Governance
- If in any doubt – **do not share** information and seek advice before proceeding further.

Declaration

I confirm that I am fully aware that I have a legal duty of confidentiality to the CCG. I further confirm that I will not disclose any unauthorised information belonging to patients, the CCG's staff or the CCG's affairs and those of other associated organisations to any other party.

I am aware that any breach of this undertaking is a serious matter that may lead to disciplinary action. The CCG may also instigate legal proceedings against an individual who does not comply with its confidentiality requirements.

There may be occasions when staff have a duty to raise concerns over health service issues and the legal duty of confidence may be overridden, i.e. a statutory requirement or in the public interest. In all cases references must be made to your line manager or senior manager who will, if necessary take further advice, before any disclosure is made.

Further information can be found in the **Information Security Policy, Email & Internet Use Policy, Disciplinary Policy and Whistleblowing Policy** which I will read as soon as possible after commencing my employment/engagement.

To confirm that I have read, fully understood and agree to abide by the above statement.

Signed: ……

Name: ……

Role: ……

Date: ……

Appendix C: Equality Impact Analysis

Equality Impact Analysis on the

Confidentiality and Safe Haven Policy

1 What is it about?	***Refer to the Equality Act 2010***
a) Describe the proposal/policy and the outcomes/benefits you are hoping to achieve The Confidentiality and Safe Haven 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.	
b) Who is it for? All staff	
c) How will the proposal/policy meet the equality duties? The policy will have no adverse effect on equality duties as it considers the confidentiality of information to be of equal status across all groups of people.	
d) What are the barriers to meeting this potential? There are no barriers.	
2 Who is using it?	***Consider all equality groups***
a) Describe the current/proposed beneficiaries and include an equality profile if possible The policy is applicable to all.	
b) How have you/can you involve your patients/service users in developing the proposal/policy? Patients and service users have not been involved in developing the policy as this is an operational policy.	
c) Who is missing? Do you need to fill any gaps in your data? There are no gaps.	
3 Impact	***Consider how it affects different dimensions of equality and equality groups*** Using the information from steps 1 & 2 above:
a) Does (or could) the proposal/policy create an adverse impact for some groups or individuals? Is it clear what this is? It is not anticipated that any adverse impact will be created.	
b) What can be done to change this impact? If it can't be changed, how can this impact be mitigated or justified? This is not applicable.	
c) Does (or could) the proposal/policy create a benefit for a particular group? Is it clear what this is? Can you maximise the benefits for other disadvantaged groups? This policy is equal across all groups.	

d) Is further consultation needed? How will the assumptions made in this analysis be tested? No.
4 So what (outcome of this EIA)? *Link to the business planning process*
a) What changes have you made in the course of this EIA? None.
b) What will you do now and what will be included in future planning? Not applicable.
c) When will this EIA be reviewed? At policy review.
d) How will success be measured? No equality issues are created.

Sign-off

Name of person leading this EIA: **Angela Sumner** **angelasumner@nhs.net**	Date completed: **08-06-18** Proposed EIA review date: **01-04-20**
Signature of director/decision-maker **Add signature** Name of director/decision-maker **Insert Name and Position**	Date signed **Insert date**