Document information

Document type:	Policy
Document reference:	
Document title:	**Confidentiality and Safe Haven Policy**
Document operational date:	
Document sponsor:	Steve Perkins, SIRO
Document manager:	Susannah Long, Governance & Risk Manager
Approving Committee/Group:	Audit and Assurance Committee
Approval date:	13 November 2018
Version:	1.0
Recommended review date:	November 2021
Internet location:	

Please be aware that this printed version of this document may NOT be the latest version. Please refer to the internet for the latest version.

Summary

This policy details how the CCG will meet its legal obligations and NHS requirements concerning confidentiality and information security standards. The policy details how procedures are used to ensure 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.

Consultation

This policy has been developed by South Central & West Commissioning Support Unit to comply with latest guidance and legislation. The policy has been adapted to reflect local CCG arrangements. Local consultation has been undertaken with members of the CCG Information Governance Group.

Review Log

Version	Review Date	Reviewed By	Changes Required? (If yes, please summarise)	Changes Approved By	Approval Date
0.1	Sept'18	Governance & Risk Manager	New document	IGG	Sept'18
1.0	Nov'18	IGG		AAC	Nov'18

Acknowledgements

Standard Confidentiality & Safe Haven Policy written and provided by South, Central & West Commissioning Support Unit in July 2018.

Confidentiality and Safe Haven Policy

Version 1.0

Version Number: 2.0	Issue/approval date: 25-06-18
Status: Final	Next review date: April 2020

Document Control

Document Name	Version	Status	Author
Confidentiality and Safe Haven Policy	2.0	Final	Information Governance Services
Document objectives:	This policy describes SCW CSU and Wiltshire CCG 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*:*	SCW Information Governance Steering Group		
Monitoring arrangements and indicators:	This policy will be monitored by the CSU 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 'Latest News' section of the intranet and the policy will be posted on the intranet with links to the IG page		
Approved and ratified by:	SCW Information Governance Steering Group Corporate Governance and Assurance Group	Date: 07-06-18 Date: 25-06-18	
Equality Impact Assessment:	Yes	Date: 08-06-18	
Date issued:	tbc		
Review date:	April 2020		
Author:	Information Governance Team		
Lead Director:	Head of Information Governance		

Version Control

Change Record

Date	Author	Version	Page	Reason for Change
12.06.15	Shelley Brown	1.2	Various	Amend to South Central and West Commissioning Support Unit
03.12.15	Shelley Brown	1.3	Various	General updates re legislation/procedures
09.08.16	Shelley Brown	1.4	5	Reference to codes of practice on confidential information
01.11.16	Shelley Brown	1.5	2	Update to IG Team inbox address
16.11.16	Hayley Matthews	1.6	6 13	Reference to Caldicott 3 added, Links to Caldicott Reports 1997, 2013 and Caldicott 3 added
11.09.17	Jackie Thomas	1.7	6	Remove reference to Operational Management Team
11.09.17	Jackie Thomas	1.7	6	Remove HSCIC and replace with NHS Digital
11.09.17	Jackie Thomas	1.7	8	Update IG Training Tool details to e-LfH
11.09.17	Jackie Thomas	1.7	9	Include GDPR review information
11.09.17	Jackie Thomas	1.7	10	NHS Mail changes to procedure
30.10.17	Jackie Thomas	1.7	Various	Remove references to the CSU and replace with SCW
	Angela Oakley	1.7	Various	Draft update in line with GDPR implementation
14-05-18	Angela Sumner & Matt Wall	V2.0	All	Review due to changes in Data Protection Legislation and amalgamation of the Safe Haven Policy

Reviewers/contributors

Name	Position	Version Reviewed & Date
Shelley Brown	Regional Information Governance Lead	V1.2 12.06.15
Shelley Brown	Regional Information Governance Lead	V1.3 03.12.15
Shelley Brown	Regional Information Governance Lead	V1.4 09.08.16
Shelley Brown	Regional Information Governance Lead	V1.5 01.11.16
Hayley Matthews	Information Governance Manager	V1.6 16.11.16

Version Number: 2.0	Issue/approval date: 25-06-18
Status: Final	Next review date: April 2020

Jackie Thomas	Information Governance Manager	V1.7 30.10.17
Angela Sumner	Senior Information Governance Manager	V1.8
Matthew Wall	Information Governance Manager	V2.0 18/05/18

Contents

Version Number: 2.0	Issue/approval date: 25-06-18
Status: Final	Next review date: April 2020

1. INTRODUCTION

Wiltshire 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 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 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.

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 CCG 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.

For specific guidance and procedures in respect of telephony enquiries, e-mails, faxes and post, please refer to the 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 organisation's IAR will be kept up to date by Information Asset Owners (IAA) / Data Custodians and remain the responsibility of the individual team Information Asset Owners (IAO) 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 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.

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 (DPO), who will provide advice and guidance and inform and obtain the 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 GDPR or support from NHS England who will apply for the necessary approval from the appropriate authority.

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 (DPO), who will provide advice and guidance in cases where a decision to share is not clear. Where necessary it may be prudent to inform and obtain the 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. 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 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 particularly overnight.

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. Data must be kept safe from damage or destruction.

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. Staff must not print out data on their home printers.

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 Accountable 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 Management Team. The SCW IG Manager is responsible for reporting Information Governance risks and issues to the Information Governance 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 IAOs and DCs/IAAs. In order that IAOs and DCs 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 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 Assistants

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 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 (DPIA)
- 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 (ConsultOD) 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.

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, available on the ConsultHR portal.

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 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 Policy is available on ConsultHR.

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 to exercise their 'right of access', as defined in the 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.
Appendix B contains an Evaluation Standard that may be used by managers to check local compliance with the policy.

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 April 2020.

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:

- 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 the Information Governance (IG) Policy, the Records Management Policy and the Staff Handbook.

APPENDIX A: 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**

APPENDIX B: EVALUATION STANDARD

Policy Name: Confidentiality & Safe Haven Policy
Policy Reference: TBC

Standard statement

This policy details how the CCG will meet its legal obligations and NHS requirements concerning confidentiality, and the procedures in place to ensure 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.

Criteria - Corporate

1. Confidentiality audits are arranged and undertaken.

2. The Data Protection Officer ensures 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.

3. All contracts of employment include a clause on adherence to the data protection legislation and the common law duty of confidentiality.

Criteria - Departmental

4. All staff are aware of the different categories of data.

5. Safe haven procedures are in place 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.

6. When sending confidential information the appropriate classification is used (Official sensitive personal / Official sensitive commercial).

7. All databases are included on the Information Asset Register.

8. All sharing of data (internal/external) is recorded appropriately on the Data Flow Map.

9. A Data Protection Impact Assessment (DPIA) is completed prior to any movement of data by electronic or physical means and prior to any sharing.

10. All contracts between the CCG and third parties contain data protection and confidentiality clauses.

11. No personal, commercially confidential or special categories of personal data should be disclosed or transferred outside of the European Economic Area (EEA)

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

13. Staff do 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. Staff must not print out data on their home printers.

14. Staff do not talk about confidential matters in public places or where they can be overheard.
15. Staff do not leave any assets containing personal, commercially confidential or special categories of personal data lying around unattended.
16. Staff do not leave their computer logged on to a system where information can be accessed or viewed by another person without authority to view that information.

17. Staff do not use someone else's password to gain access to data.

18. There are nominated Information Asset Owner(s), Data Custodian(s) and Information Asset Administrator(s) in place.

19. All staff have undertaken appropriate training and awareness in line with the CCG Training Needs Analysis (TNA).

20. All agency and non-contract staff working on behalf of NHS have a signed confidentiality agreement in place.

21. All staff are aware that 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.

Conclusion

Please explain any discrepancies below:

Please detail remedial action to prevent re-occurrence, giving details of monitoring arrangements to assess improvement:
