



West Hampshire
Clinical Commissioning Group

CONFIDENTIALITY AND SAFE HAVEN POLICY

Version 3.2

Subject and version number of document:	Confidentiality and Safe Haven Policy Version 3.2
Serial number:	COR/021/V3.02
Operative date:	1 August 2019
Author:	Information Governance Team, NHS South, Central & West Commissioning Support Unit
CCG owner:	Chief Finance Officer
Links to other CCG policies:	Risk Management Policy Individual Rights Policy Information Security Policy Remote Working & Portable Devices Policy Conduct, Performance, Grievance & Absence Management Policy
Review date:	July 2021
For action by:	All Staff
Policy statement:	This policy describes the CCG'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.
Responsibility for dissemination to new staff:	Line Managers
Mechanisms for dissemination:	This policy will be promoted through the CCG team newsletter and published on the CCG website.
Training implications:	All staff will need to be made aware of IG policies and IT security at induction, complete IG training in first year and refresher IG every year thereafter. Data custodians / information asset owners will need to undertake additional training specific to the role.
Resource implications:	There are no resource implications in relation to this policy.

Further details and additional copies available from:	Website https://westhampshireccg.nhs.uk/document-tag/ig-and-security-policies/
Equality impact assessment completed?	Yes. Neutral Impact. Risk of negative impact if policy breached. Note particular requirements of Section 22 of the Gender Recognition Act 2004.
Consultation Process	Regular review via the CCGs corporate governance meeting structure and the CSU IG Steering Group, as well as the CCG Equality & Diversity Manager.
Approved by:	Policy Sub Group
Date approved:	17 July 2019

Website Upload:

Website	Location in FOI Publication Scheme	https://westhampshireccg.nhs.uk/document-tag/ig-and-security-policies/
Keywords:	Data Protection, Information Governance, NHS Confidentiality Code of Practice, Caldicott Report 1997, 2013 and 2016	

Amendments Summary:

Amend No	Issued	Page(s)	Subject	Action Date
1	Jan 14	Pg 9	Cloud Computing added, section	3 January 2014
2	Feb 14	Pg 18	Managing protected information about transsexual people shortened.	19 February 2014
3	Nov 14	Pg 11 Pg 26	Training Equality Analysis	31 December 2014
4	Apr 16	Throughout	Update hyperlinks, amend Confidentiality agreement to bring in line with CSU Information Security Policy approved by CCG Feb 2016, amend review timescale, amend references to CSU name and Corporate Governance Committee to Finance & Assurance Committee	20 April 2016
5	Nov 16	Pg 11, 20	Included Caldicott 3 review and links to reports, changed HSCIC to NHS Digital and added additional guidance.	21 November 2016
6	Aug 17	Pg 2	Review date extended to April 2018 as agreed SIRO / Policy Sub Group September 2017. Due to the implementation of the General Data Protection Regulation all information governance policies and procedures will need to be reviewed in light of this new legislation	
7	Jun 18	Throughout	Updated by CSU re General Data Protection Regulations. CSU policy version provided / adopted (Version 2.0, 180625), amended to reflect WHCCG arrangements and to include WHCCG documentation control cover sheets rather than those of the CSU.	21 Jun 18
8	Sept 18	Throughout	Reformatted to bring in line with CCG policy template (version 3.1).	24 Sept 18
9	Jul 19	Cover Sheets and pg 20	To update version control / review log to reflect that policy was reviewed with no amendment to content required, apart from changing review timescales from annual to biennial from now on.	Jul 19

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Reviewer	Ratification Process	Notes
2	Nov 15	CSU IG Manager	Policy Sub Group, Corporate Governance Committee and then Board: January 2015	
3	Jun 18	South Central & West CSU IG Team	SIRO, Caldicott Guardian and DPO Policy Sub Group	See amend 7 above
3.2	Jul 19	South Central & West CSU IG Team	Policy Sub Group	See amend 9 above.

CONFIDENTIALITY AND SAFE HAVEN POLICY

SUMMARY OF KEY POINTS TO NOTE:

This policy describes the CCG's responsibilities under Data Protection Legislation and ensures all employees abide by the legal duty of confidence to protect personal confidential information. Specifically:

- Staff have a legal duty of confidence to keep personal confidential data private and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence. The Information Commissioners Office (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
- Staff should not: talk about personal confidential data in public places / where they can be overheard; leave any personal confidential data lying around unattended or leave a computer logged on to a system where personal confidential data can be accessed
- Personal sensitive information must not be sent to a non-secure email address
- When working away from CCG locations, staff must ensure that their working practice complies with CCG policies and procedures. Any removable media must be encrypted as per the current NHS Encryption Guidance
- 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 the CCG to ensure confidential patient or staff information is communicated safely and securely. It is a safeguard for confidential information, which enters or leaves the CCG whether this is by fax, post or other means. Any members of staff handling confidential information, whether paper based or electronic must adhere to the safe haven principles.
- No personal data should be disclosed or transferred outside of the European Economic area to a country or territory which does not ensure an adequate level of protection. Advice should be sought from the CCG data protection officer prior to any agreement to transfer or process outside of the United Kingdom.
- It is strictly forbidden for employees to knowingly browse, search for or look at any information relating to themselves, their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as breach of confidentiality and Data Protection Legislation.

CONFIDENTIALITY AND SAFE HAVEN POLICY

Contents

- 1. Introduction and Purpose 9
- 2. Scope and Definitions 9
- 3. Process / Requirements 9
- 4. Roles and Responsibilities 17
- 5. Confidentiality Audits..... 18
- 6. Training 18
- 7. Contracts of Employment 19
- 8. Disciplinary..... 19
- 9. Abuse of Privilege 19
- 10. Equality Analysis 20
- 11. Success Criteria / Monitoring the Effectiveness of the Policy 20
- 12. Review 20
- 13. References and Links to Other Documents..... 21
- Appendix A: Confidentiality Agreement template..... 23
- Appendix B: Equality Impact Analysis..... 28

CONFIDENTIALITY AND SAFE HAVEN POLICY

1. INTRODUCTION AND PURPOSE

- 1.1 West Hampshire 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.
- 1.2 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.
- 1.3 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.

2. SCOPE AND DEFINITIONS

- 2.1 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

- 2.2 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.
- 2.3 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. PROCESS / REQUIREMENTS

Security & Confidentiality

- 3.1 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

3.2

<p>Personal Data (derived from the GDPR)</p>	<p>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</p>
<p>'Special Categories' of Personal Data (derived from the GDPR)</p>	<p>'Special Categories' of Personal Data is different from Personal Data and consists of information relating to:</p> <ul style="list-style-type: none"> • 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
<p>Personal Confidential Data</p>	<p>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).</p>
<p>Protected Information</p>	<p>Managing protected information about transsexual people. Section 22 of the Gender Recognition Act 2004 says that:</p> <p>'It is an offence for a person who has acquired protected information in an official capacity to disclose the information to any other person.'</p>

	'Protected information' means information which relates to a person who has made an application under the Gender Recognition Act. This covers both the fact of the application itself and, if the application was successful, the fact that the individual was previously of the opposite gender to the one in which they are now legally recognised. See Appendix 1 for more information.
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

- 3.3 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

- 3.4 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.
- 3.5 NHS England and other NHS / public bodies have adopted the Government Security Classifications, published April 2014 i.e.

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

- 3.6 Whilst the CCG has not yet adopted the Protective Marking Scheme, any information received from an NHS organisation marked as OFFICIAL-SENSITIVE (PERSONAL or COMMERCIAL) should be treated as Confidential. Please refer to the Records Management Policy for further information.

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

Database Management

- 3.8 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.
- 3.9 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

- 3.10 SCW IT Services Teams are responsible for ensuring that appropriate back up procedures are available and implemented under the service level agreements in place for the systems they manage and service.

Disclosure of Information & Information Flows

- 3.11 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.
- 3.12 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.
- 3.13 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).
- 3.14 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.
- 3.15 Contracts between the CCG and third parties must include appropriate Data Protection and Confidentiality clauses.

- 3.16 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)

- 3.17 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.
- 3.18 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

- 3.19 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.
- 3.20 It is important to consider how much data is required and ensure that the minimal amount necessary is disclosed.
- 3.21 Data can be disclosed when effectively anonymised/pseudonymised in line with legislative requirements and the ICO Anonymisation Code of Practice.
- 3.22 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.
- 3.23 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 for example, the Confidentiality Advisory Group (CAG).
- 3.24 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 the safeguarding adults team,

the safeguarding children team, the Caldicott guardian or the data protection officer who will provide advice and guidance and in cases where a decision to share is not clear (please refer to the CCG Safeguarding Adults and Safeguarding Children policies. Where necessary approval may need to be obtained from the Caldicott guardian for the disclosure.

- 3.25 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.
- 3.26 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.
- 3.27 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.
- 3.28 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.
- 3.29 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.
- 3.30 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](#).
- 3.31 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.
- 3.32 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.
- 3.33 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
- Care Act 2014
- Gender Recognition Act 2004

3.34 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

3.35 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.

3.36 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.

3.37 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.

3.38 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.

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

- 3.40 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. in 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.
- 3.41 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.
- 3.42 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 or approved for use by the CCG.

Use of cloud technology

- 3.43 Before considering whether a cloud service or cloud provider is right for the CCG, consideration should be given to how it is intended to process personal or commercially confidential data in the cloud.
- 3.44 Once the CCG is clear which personal or commercially confidential data it holds and how it intends to process it in the cloud, the associated risk should be assessed and appropriate steps taken to mitigate them. A clear record about the categories of data the CCG intends to move to the cloud should be kept.
- 3.45 If services within the CCG are looking to process personal data in a cloud service, a data protection impact assessment should be carried out in order to assess and identify any privacy concerns and address them at an early stage. The CCG senior information risk owner (SIRO), Caldicott guardian and data protection officer should be involved in this process and the decision to proceed should be approved by the appropriate senior management or committee.
- 3.46 Data Protection Legislation requires the CCG, as data controller, to have a written contract with the data processor (cloud provider) which clearly requires the data processor to act only on instructions from the data controller and also requires the data processor to comply with security obligations equivalent to those imposed on the CCG itself.
- 3.47 The existence of a written contract should mean that the cloud provider will not be able to change the terms of data processing operations during the lifetime of the contract without the CCG's knowledge and agreement.
- 3.48 As a data controller, the CCG should ensure appropriate steps are taken to inform the public of the use of the cloud service if any personal identifiable data is to be stored by this method. This should be done via the CCG fair processing notification which should be available on the CCG public website.

- 3.49 Further information regarding the use of the cloud can be found on the Information Commissioners Office website at [ICO - Cloud Computing](#).

4. ROLES AND RESPONSIBILITIES

Chief Officer

- 4.1 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 Audit Committee.

Audit Committee

- 4.2 The Audit Committee is responsible for reporting Information Governance risks and issues to the CCG Board.

Data Protection Officer

- 4.3 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.

Information Asset Owners (IAOs) / Data Custodians (DCs)

- 4.4 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.

Staff

- 4.5 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
- 4.6 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.

- 4.7 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. CONFIDENTIALITY AUDITS

- 5.1 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. TRAINING

Information Asset Owner, Data Custodians/Information Asset Administrators

- 6.1 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
 - The IAO/Data Custodian work programme

All Staff

- 6.2 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.
- 6.3 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.
- 6.4 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.
- 6.5 Please see IG Services Incident Management and Reporting Procedure for further guidance on this area.

7. CONTRACTS OF EMPLOYMENT

- 7.1 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.
- 7.2 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.

8. DISCIPLINARY

- 8.1 A breach of the Data Protection Legislation requirements could result in a member of staff facing disciplinary action. Please refer to the CCG Conduct, Performance, Grievance & Absence Management Policy: Disciplinary Procedure.

9. ABUSE OF PRIVILEGE

- 9.1 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.

- 9.2 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.

10. EQUALITY ANALYSIS

- 10.1 An Equality Impact Analysis (EIA) has been completed by SCW CSU using their template. 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
- 10.2 However, there is a risk of negative impact if the policy is breached; note particular requirements of Section 22 of the Gender Recognition Act 2004 (see Section 3 of this policy). A copy of the EIA is attached at Appendix B.

11. SUCCESS CRITERIA / MONITORING THE EFFECTIVENESS OF THE POLICY

- 11.1 This policy will be monitored by the SCW IG Team to ensure any legislative changes that occur before the review date are incorporated. Compliance and effectiveness with IG policies/guidance will be monitored through the following mechanisms:
- Receipt of the IG Staff Handbook confirmation slips confirming staff have received a copy of the handbook and understand their responsibilities
 - Completion of induction and annual IG training which is monitored via the E-Learning for Health IG training tool
 - Completion of IG modules / training relevant to the roles of the Senior Information Risk Owner, Caldicott Guardian, Data Protection Officer, Information Asset Owners and Information Asset Administrators
 - Regular IG reports to the CCG Audit Committee
 - Updates to the West Hampshire IG Group
 - Annual submission of evidence to the Data Security and Protection Toolkit (DSP Toolkit)
 - Annual audit by the CCG's internal auditors
- 11.2 Please refer to Individual Rights policy for guidance on how to handle a 'Right of Access' Subject Access Request or Access to Records requests.

12. REVIEW

- 12.1 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 by SCW CSU in June 2021.

13. REFERENCES AND LINKS TO OTHER DOCUMENTS

13.1 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
- Care Act 2014
- Gender Recognition Act 2004
- The Privacy and Electronic Communications (EC Directive) Regulations 2003

13.2 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

13.3 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 – West Hampshire CCG

Document name	Confidentiality Agreement	
Date:	XX/XX/20XX	
Author	Information Governance Team, NHS South, Central and West CSU	
Version	2	

Confidentiality agreement for third party suppliers

Who are third parties covered by this agreement?

Third party suppliers granted access to West Hampshire CCG 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, 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 SCW 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 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: Equality Impact Analysis

Equality impact assessment

Title of policy, project or proposal:
Confidentiality and Safe Haven Policy

Lead manager:	Senior Information Risk Owner
Directorate:	Finance & Performance

What are the intended outcomes of this policy, project or proposal?
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.

Evidence
Who will be affected by the policy, project or proposal? Staff, patients and carers
Age Neutral impact. Negative impact if this and related policies are not followed.
Disability Neutral impact. Negative impact if this and related policies are not followed.
Dementia Neutral impact. Negative impact if this and related policies are not followed.
Gender reassignment (including transgender) Neutral impact. Negative impact if this and related policies are not followed. Note particular requirements under Section 22 of the Gender Recognition Act 2004 outlined in Section 3 of this policy.
Marriage and civil partnership N/A
Pregnancy and maternity Neutral impact. Negative impact if this and related policies are not followed.

Race

Neutral impact. Negative impact if this and related policies are not followed.

Religion or belief

Neutral impact. Negative impact if this and related policies are not followed.

Sex (gender)

Neutral impact. Negative impact if this and related policies are not followed.

Sexual orientation

Neutral impact. Negative impact if this and related policies are not followed.

Carers

Neutral impact. Negative impact if this and related policies are not followed.

Serving Armed Forces personnel, their families and veterans

Neutral impact. Negative impact if this and related policies are not followed.

Other identified groups

Neutral impact. Negative impact if this and related policies are not followed.

Involvement and consultation

For each engagement activity, briefly outline who was involved, how and when they were engaged, and the key outputs

How have you involved stakeholders with an interest in protected characteristics in gathering evidence or testing the evidence available?

Not applicable.

How have you involved/ will you involve stakeholders in testing the policy, project or proposals?

Not applicable.

Equality statement

Considering the evidence and engagement activity you listed above, please summarise the findings of the impact of your policy, project or proposal. Consider whether the evidence shows potential for differential impact, if so state whether adverse or positive and for which groups.

Impact summary (statutory considerations)

Age	Positive	Neutral	Negative
Disability	Positive	Neutral	Negative
Sexual orientation	Positive	Neutral	Negative
Race	Positive	Neutral	Negative
Religion or belief	Positive	Neutral	Negative
Gender reassignment	Positive	Neutral	Negative
Sex	Positive	Neutral	Negative
Marriage and civil partnership	Positive	Neutral	Negative
Pregnancy and maternity	Positive	Neutral	Negative

Other policy considerations

Poverty	Positive	Neutral	Negative
Place (Rural versus urban living)	Positive	Neutral	Negative
Serving Armed Forces/ veterans	Positive	Neutral	Negative
Other factors	Positive	Neutral	Negative

Have you identified any positive or negative impacts?

Yes No

If 'Yes' please provide details below

Positive impacts

Not applicable.

Negative impacts

Breaches of this policy could have a negative impact.

Health inequalities

Not applicable.

Action planning for improvement, and to address health inequalities and discrimination

Please give an outline of the key actions based on any gaps, challenges and opportunities you have identified. Include here any general action to address specific equality issues and data gaps that need to be addressed through consultation or further research.

Action	Person responsible	By date
1. To ensure that the policy takes account of equalities monitoring and the confidentiality requirements defined in the Gender Recognition Act 2004.	Information Governance Manager / SIRO	Completed as part of policy review.

For your records

Person who carried out this assessment:	CSU IG Team
Date assessment completed:	8 June 2018
Date to review actions:	Not applicable
Responsible Director:	Chief Finance Officer (SIRO)
Date assessment was approved:	18 July 2018 via Policy Sub Group