NHS
Cambridgeshire and
Peterborough
Clinical Commissioning Group

Cambridgeshire and Peterborough Clinical Commissioning Group

SAFE HAVEN POLICY 2021-2023

Approval Process

Lead Author:	CCG IG Lead / Data Protection Officer
Reviewed by:	CCG IG, BI and IM&T Steering Group
Approved by:	CCG IG, BI and IM&T Steering Group – 14th October 2021
Ratified by:	Integrated Performance and Assurance Committee (IPAC)
Date Ratified:	23rd November 2021
Version:	5.0
Review date:	July 2023 (or earlier if significant change to local or national requirements)
Valid on:	23rd November 2023

Document Control Sheet

Development and Consultation:	Policy developed by CCG IG Lead / Data Protection Officer, in consultation with the IG, BI & IM&T Steering Group and ratified by Integrated Performance and Assurance Committee.
Dissemination	This policy will be promoted and available to all staff within the CCG.
Implementation	The Chief Finance Officer (SIRO) is responsible for monitoring the application of the policy by ensuring that: • The policy is brought to the attention of all employees and building users • Managers are aware of their responsibilities for ensuring that staff under their control implement and adhere to the policy • Staff are informed and consulted as appropriate • Appropriate training and guidance is provided to staff • Corporate business processes support the implementation of the policy.
Training	Training will be undertaken as part of the CCG's on-going processes.
Audit	Implementation of the Policy will be monitored in line with Data Security and Protection Toolkit requirements
Review	This policy will be reviewed two yearly, or earlier if there are changes in procedures or legislation.
Links with other Documents	The Policy should be read in conjunction with: • Information Governance Policy • Cambridgeshire and Peterborough Information Sharing Framework • Information Security for Staff Policy • NHS Code of Confidentiality • CCG Code of Conduct for Confidentiality • CCG Records Management and Lifecycle Policy • CCG Removable Media Policy
Equality and Diversity	The OD & HR Advisor (Equality and Diversity) has carried out an Equality & Diversity Impact assessment (Annex A) and concluded that the policy is compliant with the CCG Equality and Diversity Policy. No negative impacts were found.

Revisions

Version	Page/ Para No	Description of change	Date approved
1	Whole document	Development of policy for Cambridgeshire and Peterborough CCG	April 2013
1.1	Appendices 3 & 4	Fax header sheets amended	September 2013
1.2	Links with other Documents	Updated policy list	November 2013
2.0	Whole document	Reviewed and ratified by CMET	July 2015
3.0	Whole document	Business Intelligence inclusion, Information Sharing Protocol is now the county wide Information Sharing Framework, addition of 7th Caldicott Principle Addition of 2.2. Section 4 updated. Section 7.3 added	May 2017
4.0	Whole document	Bi-annual review and update. Changes to reporting Committee and references to GDPR / DPA 2018 and Toolkit. Faxing section updated in accordance with the NHS Health and Social Care Secretary's national mandate to cease NHS use of Fax by 1st April 2020.	October 2019
5.0	Whole document	Biennial review and update.	October 2021

Table of Contents

1. Purpose

1.1. All NHS organisations require safe haven procedures to maintain the privacy and confidentiality of person identifiable information held. The implementation of these procedures facilitates compliance with the legal requirements placed upon the organisation, especially concerning sensitive information e.g. a person's medical condition.

1.2. Where Trusts and external partner agencies want to send person identifiable information to NHS Cambridgeshire and Peterborough CCG ('the CCG') department, they should be confident that they are doing so to a location that maintains the security of the data.

2. Scope

2.1 This policy provides:

- The legislation and guidance that dictates the need for a safe haven;
- A definition of the term 'safe haven';
- Outlines when a safe haven is required
- The necessary procedures and requirements that are needed to implement a safe haven;
- Rules for different kinds of safe haven;
- Sets out access disclosure rules.

2.2 This policy applies to all CCG staff and includes but is not limited to governing body members, contractors, agency and temporary staff, student, honorary and volunteer staff. It is applicable to all areas of the CCG and adherence should be included in all contracts for commissioned or collaboratively commissioned services, without exception.

3. Legislation and guidance

3.1 A number of Acts; guidance and principles dictate the need for safe haven arrangements to be set in place, they include:

A key principle of the **Data Protection Act 2018** (the UK's implementation of the General Data Protection Regulation (GDPR)) is that organisations process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.

NHS Digital Code of practice on confidential information **–** Annex 1 - Protect patient information; '*Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring from one location to another are secure as they can be.' (See Appendix 3)*

NHS Digital's Data Security and Protection Toolkit requires organisations to have a documented plan to ensure that transfers of person identifiable and sensitive information are adequately secure.

Caldicott Principles

The Caldicott Principles are eight principles to ensure people's information is kept confidential and used appropriately.

Good information sharing is essential for providing safe and effective care. There are also important uses of information for purposes other than individual care, which contribute to the overall delivery of health and social care or serve wider public interests.

These principles apply to the use of confidential information within health and social care organisations and when such information is shared with other organisations and between individuals, both for individual care and for other purposes.

The principles are intended to apply to all data collected for the provision of health and social care services where patients and service users can be identified and would expect that it will be kept private. This may include for instance, details about symptoms, diagnosis, treatment, names and addresses. In some instances, the principles should also be applied to the processing of staff information.

They are primarily intended to guide organisations and their staff, but it should be remembered that patients, service users and/or their representatives should be included as active partners in the use of confidential information.

Where a novel and/or difficult judgment or decision is required, it is advisable to involve a Caldicott Guardian.

Principle 1: Justify the purpose(s) for using confidential information
Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2: Use confidential information only when it is necessary
Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information
Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strict need-to-know basis.
Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: **Everyone with access to confidential information should be aware of their responsibilities**
Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6: Comply with the law
Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality
Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8: Inform patients and service users about how their confidential information is used
A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

4. Definitions

4.1. **Safe haven** – The term safe haven is recognised throughout the NHS to describe the administrative arrangements to safeguard the confidential transfer of person identifiable information between organisations or sites. This term was initially meant to describe the transfer of facsimile messages, but with use of these being phased out, should now cover the data held and used within:

- Post
- Telephones, answer machines
- Digital and manual records and books
- White boards / notice boards
- Emails
- Bulk data transfers (*See Appendix 3*)

4.2. **'Person Identifiable' Information**
The General Data Protection Regulation (Article 4) defines 'personal data' as:

'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',

4.3. ‘Sensitive Person Identifiable’ Information (Special Category Data)

This is information that contains sensitive personal detail and is a subset of Personal Data. Sensitive personal information is personal data consisting of information as to a data subject’s:

(a) racial or ethnic origin;
(b) political opinions;
(c) religious beliefs or other beliefs of a similar nature;
(d) whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) physical or mental health or condition;
(f) sexual life;
(g) the commission or alleged commission of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

4.4. Confidential Personal Information

Confidential Patient Information is a legal term in use across the health and care system. It is defined in section 251(11) of the National Health Service Act 2006. Section 251 has been updated to ensure that the definitions used expressly include local authority social care, that is care provided for, or arranged by, a local authority. Broadly it is information about either a living or deceased person that meets the following 3 requirements:

- identifiable or likely identifiable e.g. from other data likely to be in the possession of the data recipient; and
- given in circumstances where the individual is owed an obligation of confidence; and
- conveys some information about the physical or mental health or condition of an individual, a diagnosis of their condition; and/or their care or treatment.

4.5 **Business Sensitive information** – This is information that if disclosed could harm or damage the reputation or image of an organisation.

5. Identifying when safe haven procedures should be in place

5.1. Safe haven procedures should be in place in any location where large amounts of person identifiable information is received, held, or communicated, especially where the person identifiable information is of a sensitive nature.

6. Requirements for safe havens

6.1 Location / security arrangements:

- It should be in a room that is locked or accessible via a coded keypad known only to authorised staff, **or**
- The office or workspace should be sited in such a way that only authorised staff can enter that location, i.e. it is not an area which is readily accessible to other members of staff who work in the same building or office, or any visitors.
- If sited on the ground floor any windows should have locks on them.
- The room should conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage.
- Manual paper records containing person identifiable information should be stored in locked cabinets. Desks should be kept clear and all person identifiable data locked away at the end of the day.
- Desktop or laptop devices should not be left on view or accessible to unauthorised staff and should have a secure screen saver function and be switched off when not in use.

7. Rules for different kinds of safe haven

All points of receipt of information should be given safe haven consideration by staff including phone messages, electronic mailboxes, pigeonholes and in-trays for paper information, notice boards etc.

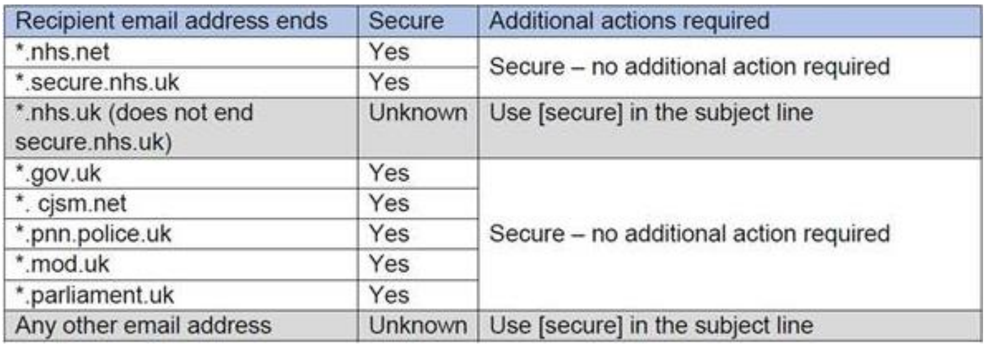
All staff should be alert to the need to protect confidential information should it come their way. For guidance on what can be shared and how, staff should refer to the CCG's Data Protection Policy; Access to Records Policy and the Cambridgeshire and Peterborough Health and Social Care Information Sharing Framework or contact the CCG's IG team or Caldicott Guardian.

7.1 **By Telephone** *(See Appendix 2)*
For incoming calls where person identifiable information is shared with someone unknown the following practice must be adhered to:

- Confirm the name, job title, department and organisation of the person requesting information;
- Confirm the reason for request, if appropriate;
- Take a contact telephone number, e.g. main switchboard number
- Check whether the information can be provided. If in doubt tell the enquirer you will call them back;
- Provide the information only to the person who has requested it (do not leave messages);
- Ensure that you record your name, the date and time of disclosure, the reason for it and who authorised sharing. Also record the recipient's named, job title, organisation and telephone number;
- Staff are expected to apply common sense with regard to the open plan office and use an available private room for telephone conversations that are highly confidential.

7.2 **By Email**

NHS mail is currently the only NHS approved method for exchanging person identifiable or sensitive data, but only if both the sender and recipient use an NHS mail account or if sending to another government secure domain. The table below is a summary of email addresses that are known or not known to be secure but please refer to NHS Guidance for sending secure email for the latest guidance.



Recipient email address ends	Secure	Additional actions required
*.nhs.net	Yes	Secure – no additional action required
*.secure.nhs.uk	Yes	
*.nhs.uk (does not end secure.nhs.uk)	Unknown	Use [secure] in the subject line
*.gov.uk	Yes	Secure – no additional action required
*. cjsm.net	Yes	
*.pnn.police.uk	Yes	
*.mod.uk	Yes	
*.parliament.uk	Yes	
Any other email address	Unknown	Use [secure] in the subject line

All person identifiable information received should be stored appropriately on receipt. For example, saved to folders with restricted access (available only to authorised members of staff) or details should be transferred into the relevant database or health record and the original email deleted.
Please refer to the CCG's Staff Information Security Policy.

7.3 **Email encryption**

The NHS mail encryption feature means that NHS mail users can also securely exchange sensitive information with users of non-accredited or non-secure email services, for example those ending in nhs.uk, Hotmail, Gmail and Yahoo. The NHS mail encryption feature means that health and social care staff now benefit from a secure service which allows them to communicate across organisation boundaries and industry sectors. NHS mail can now be used securely across the entire health and social care community – in fact with anyone using any email account.

With the NHS mail encryption feature:

- NHS mail users can easily communicate securely with users of ANY email service including those ending nhs.uk without having to manually encrypt sensitive information
- Users can send attachments which will automatically be encrypted for you and remain secure
- Organisations can save money by replacing existing post, fax and phone-based processes with secure email
- Users of non-accredited or non-secure email services can communicate securely with NHS mail users saving time and money, speeding up communications and improving patient care
- Communication is faster, easier and more reliable.

For NHS mail users:

If you have a contact that uses a non-accredited or non-secure email service (e.g. ending nhs.uk) with whom you need to exchange sensitive information, you will need to set up the communications channel with them first by sending the initial encrypted email that they can then open, read and reply to securely. Download the full step-by -step guidance for senders.

For non-NHS mail users:
In order to send an encrypted email to an NHS mail user, they must email you first. You can then reply to or forward their email and it will remain encrypted. You can also include attachments.

When you've received an encrypted email from an NHS mail user, in order to open it, read it and reply you will need to register for an account with the NHS mail encryption provider. Step-by-step instructions can be found in the guidance for recipients.

Users of the NHS mail email encryption service must note the following:

- Before you send an encrypted email, talk to the person you're sending it to – make sure that they're expecting the information and are ready to deal with it appropriately;
- It's your responsibility to safeguard any sensitive data you receive – if you are receiving the information on behalf of an organisation, you should do so in line with local data protection and information governance policies;
- If you are sending information to a patient, gain consent from them before you communicate with them via NHS mail and do so in line with your local information governance policies;
- Email delivery to Internet email addresses (e.g. Hotmail.com) can be unreliable. Sometimes messages are silently lost or sometimes a delivery notification is returned even if the message has not been received by the recipient. Where delivery assurance is required please ask the sender to reply to you confirming receipt.

7.4 Fax (facsimile) machines

Use of Fax Machines was banned in the NHS from 1st April 2020. From this date, NHS organisations were required to use modern communication methods, such as secure email, to improve patient safety and cyber security. Organisations are to be monitored on a quarterly basis until they declare themselves ‘fax free’. This was part of the Health and Social Care Secretary’s tech vision, to modernise the health service and make it easier for NHS organisations to introduce innovative technologies.

All CCG Teams must ensure that any reference to CCG fax numbers is removed from their document templates and email signatures.

7.5 By Post *(See Appendix 1)*

- All sensitive documents must be stored face down in public areas and not left unsupervised at any time.
- Recipients of frequent or significant numbers of confidential mail are advised to keep a log to record receipt and transfer within the organisation.
- Incoming mail should always be opened away from public areas.
- Confirm the name, department and address for the recipient. Do not use acronyms as they can be easily confused.

- Outgoing mail (both internal and external) must be sealed securely and the envelope marked ‘Private and Confidential, Addressee only’.
- For highly sensitive information courier or special delivery should be used and signed confirmation of receipt obtained.
- In general consideration should be given to transit method and distance when choosing suitable secure packaging material.
- In all cases the addressee or recipient should acknowledge receipt of the information.

7.6 Transfer of confidential hardcopy information *(See Appendix 3)*

- Lockable crates must be used to move bulk confidential hard copy information from one place to another. Hardcopy information must be stored in a locked cupboard or cabinet.
- Obtain a receipt for hand delivered confidential information.
- Person identifiable information should only be taken off site when absolutely necessary, or in accordance with local policy.
- Record what information you are taking off site and why, and if applicable, where and to whom you are taking it.
- Information must be transported in a sealed container.
- Never leave person identifiable information unattended.
- Ensure the information is returned as soon as possible.
- Record that the information has been returned.

7.7 Use of Couriers and Taxis to transport confidential information

- Only companies that hold an existing service level agreement with the organisation with an appropriate confidentiality clause can be used to transport Trust patients, staff, equipment or documentation – advice should be sought from the Information Governance Team if the name and contact details of the company are not known. Any items for transport in this way should be signed in and out appropriately and copy evidence of sending/receipt retained.

7.8 Transferring confidential information by removable media

Please refer to the CCG’s Removable Media Policy.

8. Use of Computers

- Access to any computer must be password protected in line with current IT access rules; this password must not be shared.
- Computer screens must not be left on view so members of the general public or staff who do not have a justified need to view the information can see person identifiable data. Press the Windows key and ‘L’ together to lock your computer when away from your desk. Computers or laptops not in use should be switched off or have a secure screen saver device in use.
- Information should be held on the organisation’s network servers, and not stored on local hard drives. Departments should be aware of the high risk of storing information locally and take appropriate security measures.
- Information should not be saved or copied into any PC or media that is “outside the NHS”.
- Personal information should be sent over NHS mail with appropriate safeguards:

- Clinical information is clearly marked as confidential;
- Emails are sent to the right people;
- Browsers are safely set up so that for example, passwords are not saved, and temporary internet files are deleted on exit;
- The receiver is ready to handle the information in the right way;
- Information sent by email will be safely stored and archived as well as being incorporated into patient records;
- There is an audit trail to show who did what and when;
- There is adequate fall back and fail-safe arrangements.

9. Safe haven printers

There are no designated safe haven printers, however, CCG printers have a ‘secure print’ function to print confidential documents e.g. Multi-Functional Devices (MFDs). If a printer fault develops whilst staff are using the MFDs, they must ensure that the fault is cleared before leaving the device, otherwise the documents will be printed out and available to the next user of the device once the fault has been cleared.

Where secure print is not possible, staff must ensure confidential printing is collected immediately. Confidential printing that is left lying around should be reported to the Information Governance team.

10. Sharing information with non-NHS organisations

10.1 Staff authorised to disclose information to other organisations outside the NHS must seek assurance that these organisations have a designated safe haven point for receiving person identifiable information.

10.2 NHS Cambridgeshire and Peterborough CCG must be assured that these organisations are able to comply with the safe haven ethos and meet certain legislative and related guidance requirements:

- Data Protection Act 2018
- Common law duty of confidence
- NHS Digital Code of Practice on Confidential Information

10.3 Staff sharing person identifiable information with other agencies should do so in compliance with the policies listed on this Policy’s Document Control Sheet.

11. Roles and Responsibilities

It is recognised that all staff in the organisation have responsibility for ensuring the safe receipt, maintenance and disclosure of person identifiable information and that it is done in line with this policy and that good practice is maintained throughout the organisation.

Caldicott Guardian is responsible for ensuring person identifiable information is received, stored and used in line with the Trust obligations to the Data Protection legislation and the NHS Digital Data Security and Protection Toolkit (DSPT).

SIRO (Senior Information Risk Owner) is responsible for protecting data and managing information risks.

Chief Officers and Senior Leadership Team are responsible for ensuring CCG safe haven procedures are known and followed in their areas.

All CCG staff that process person identifiable information are responsible for ensuring safe haven guidance is adhered to.

Confidentiality breaches should be reported immediately to the line manager and Information Governance Team prior to entry onto the Datix system.

12. Monitoring and Assurance

- The IG, BI and IM&T Steering Group will review Incident Reporting as a standing item on its agenda.

- The SIRO will escalate information risks to the Governing Body.

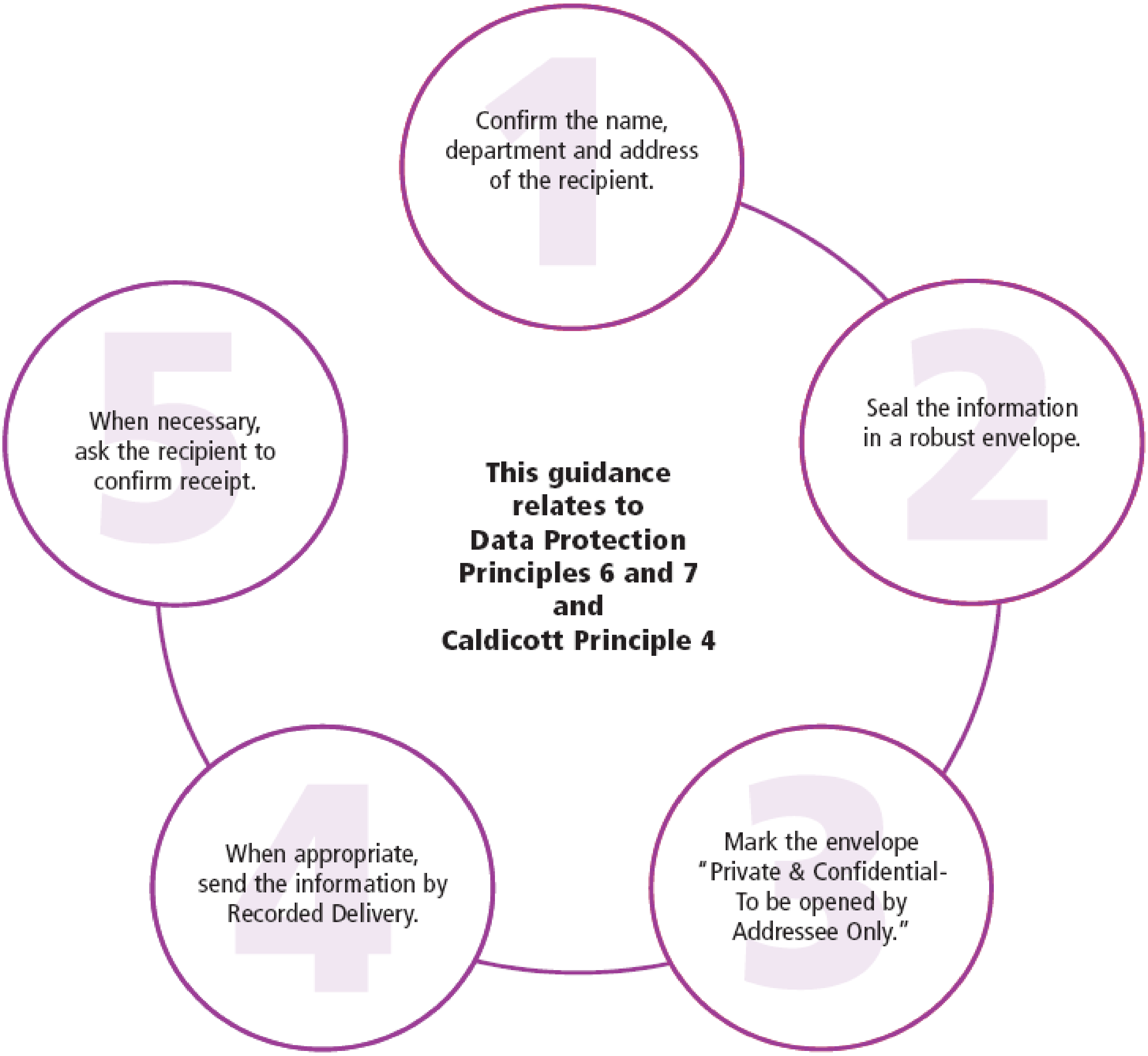
- There is an annual programme of internal and external audits in place which provides validation and assurance of the CCG's information governance systems.

- NHS Cambridgeshire and Peterborough CCG use a complaints system to effectively respond to complaints in connection with the Data Protection Act and Information Governance.

- Data Security Awareness training compliance is regularly reviewed by the CCG Integrated Performance and Assurance Committee.

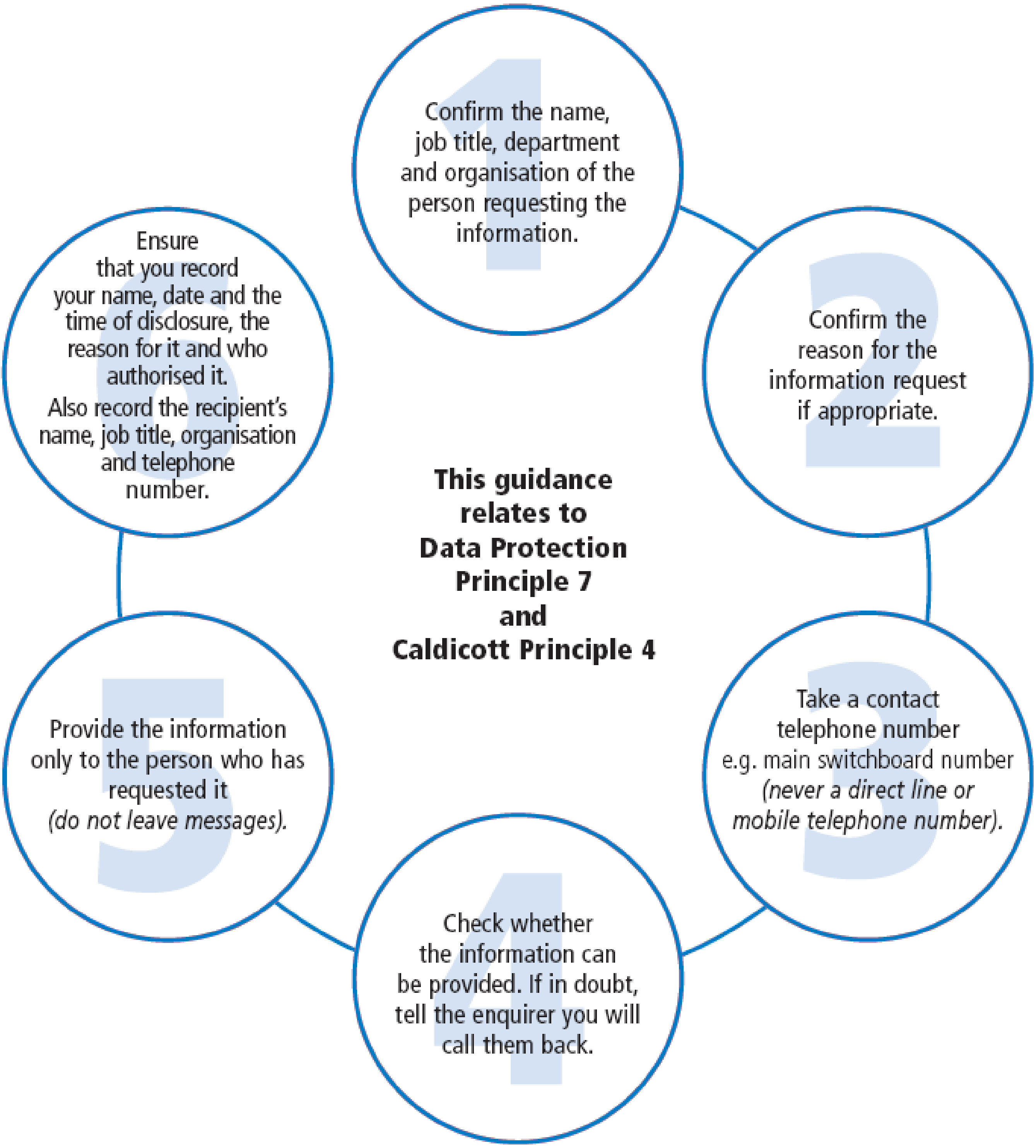
Appendix 1 – Guidance for sharing person identifiable information by post

Guidance for sharing person identifiable information by POST


1
Confirm the name, department and address of the recipient.
2
Seal the information in a robust envelope.
3
Mark the envelope "Private & Confidential- To be opened by Addressee Only."
4
When appropriate, send the information by Recorded Delivery.
5
When necessary, ask the recipient to confirm receipt.
This guidance relates to Data Protection Principles 6 and 7 and Caldicott Principle 4

Appendix 2 – Guidance for sharing person identifiable information by phone

Guidance for sharing person identifiable information by PHONE



1. Confirm the name, job title, department and organisation of the person requesting the information.

2. Confirm the reason for the information request if appropriate.

3. Take a contact telephone number e.g. main switchboard number *(never a direct line or mobile telephone number).*

4. Check whether the information can be provided. If in doubt, tell the enquirer you will call them back.

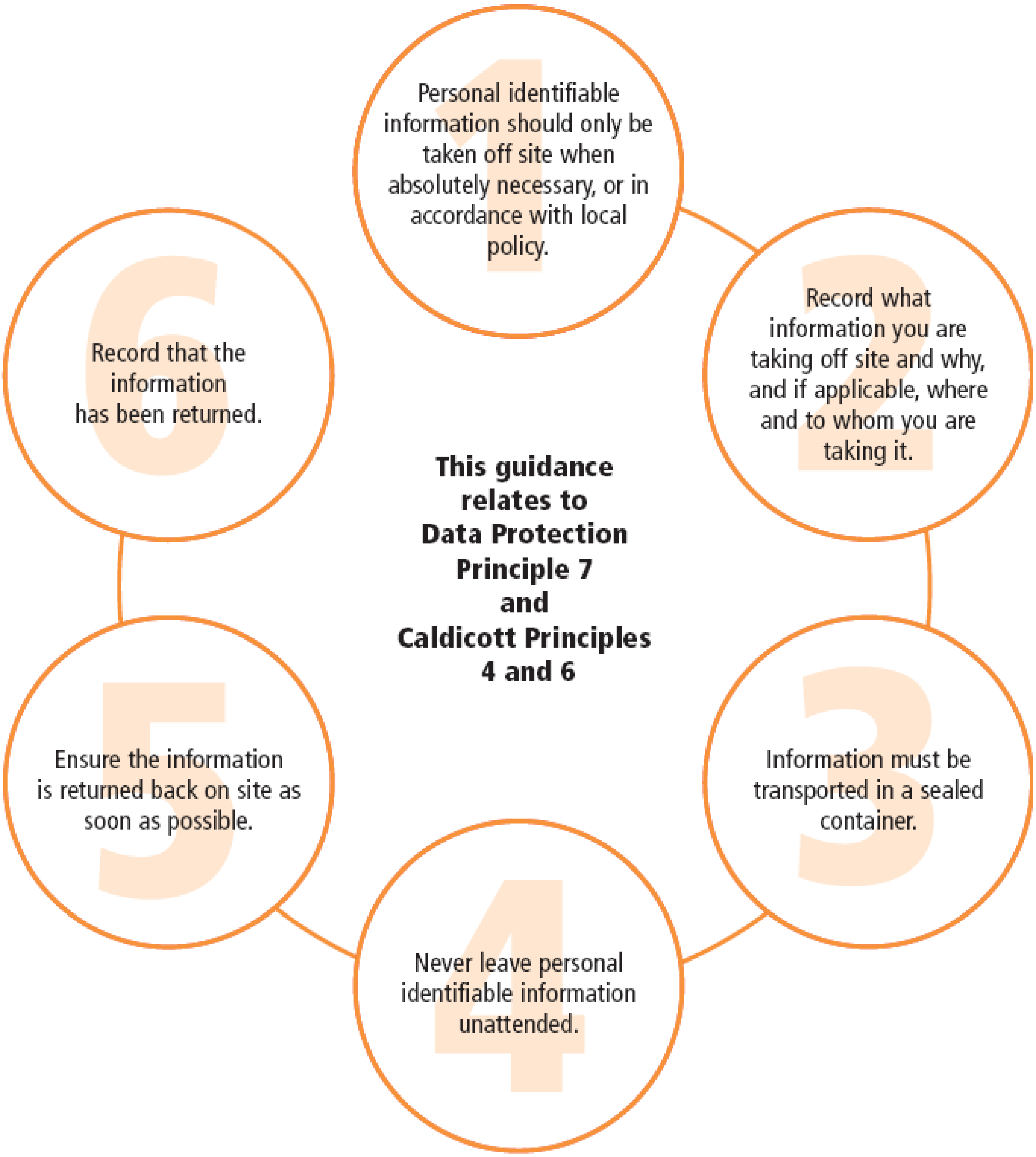
5. Provide the information only to the person who has requested it *(do not leave messages).*

6. Ensure that you record your name, date and the time of disclosure, the reason for it and who authorised it. Also record the recipient's name, job title, organisation and telephone number.

This guidance relates to Data Protection Principle 7 and Caldicott Principle 4

Appendix 3 – Guidance for transporting person identifiable information

Guidance for TRANSPORTING person identifiable information



1 Personal identifiable information should only be taken off site when absolutely necessary, or in accordance with local policy.

2 Record what information you are taking off site and why, and if applicable, where and to whom you are taking it.

3 Information must be transported in a sealed container.

4 Never leave personal identifiable information unattended.

5 Ensure the information is returned back on site as soon as possible.

6 Record that the information has been returned.

This guidance relates to Data Protection Principle 7 and Caldicott Principles 4 and 6

Annex A - Equality Impact Assessment Form

NHS
Cambridgeshire and Peterborough
Clinical Commissioning Group

Equality Impact Assessment Form

Initial Screening

Name of Proposal (policy/strategy/function/ service being assessed)	CCG Safe Haven Policy
Those involved in assessment:	Policy developed in consultation with the IG, BI & IM&T Steering Group and for endorsement by the Integrated Performance and Assurance Committee
Is this a new proposal?	No, review and revision of existing policy.
Date of Initial Screening:	April 2013
What are the aims, objectives?	All NHS organisations require safe haven procedures to maintain the privacy and confidentiality of person identifiable information held. The implementation of these procedures facilitates compliance with the legal requirements placed upon the organisation, especially concerning sensitive personal information.
Who will benefit?	All staff working for and on behalf of the CCG
Who are the main stakeholders?	Staff; Managers; IG, BI, IM&T Steering Group
What are the desired outcomes?	Staff awarenenss of the Policy through being advised of its availability on the CCG's website via iConnect.
What factors could detract from the desired outcomes?	Lack of awareness of the existence of the Policy; Failure by staff to follow the Policy.
What factors could contribute to the desired outcomes?	Knowledge of the policy and implementation
Who is responsible?	Staff, managers, IG, BI, IM&T Steering Group
Have you consulted on the proposal? If so with whom? If not, why not?	Policy developed in consultation with the IG, BI & IM&T Steering Group for approval and endorsement by the Integrated Performance and Assurance Committee.

Which protected characteristics could be affected and be disadvantaged by this proposal (Please tick)		**Yes**	**No**
Age	Consider: Elderly, or young people		X
Disability	Consider: Physical, visual, aural impairment, Mental or learning difficulties		X
Gender Reassignment	Consider: Transsexual people who propose to, are doing or have undergone a process of having their sex reassigned		X
Marriage and Civil Partnership	Consider: Impact relevant to employment and /or training		X
Pregnancy and maternity	Consider: Pregnancy related matter/illness or maternity leave related mater		X
Race	Consider: Language and cultural factors, include Gypsy and Travellers group		X
Religion and Belief	Consider: Practices of worship, religious or cultural observance, include non-belief		X
Sex /Gender	Consider: Male and Female		X
Sexual Orientation	Consider: Know or perceived orientation		X

What information and evidence do you have about the groups that you have selected above?
The above protected characteristics will have no adverse impact as the Policy has been developed in accordance with new Data Protection legislation (ie General Data Protection Regulation May 2018).

Consider: Demographic data, performance information, recommendations of internal and external inspections and audits, complaints information, JNSA, ethnicity data, audits, service user data, GP registrations, CHD, Diabetes registers and public engagement/consultation results etc.

How might your proposal impact on the groups identified? For example, you may wish to consider what impact it may have on our stated goals: Improving Access, Promoting Healthy Lifestyles, Reducing Health Inequalities, Supporting Vulnerable People

Examples of impact re given below:

a) Moving a GP practice, which may have an impact on people with limited mobility/access to transport etc

b) Planning to extend access to contraceptive services in primary care without considering how their services may be accessed by lesbian, gay, bi-sexual and transgender people.

c) Closure or redesign of a service that is used by people who may not have English as a first language and may be excluded from normal communication routes.

Summary	
Positive impacts (note the groups affected)	Negative impacts (note the groups affected)
N/A	N/A

Summarise the negative impacts for each group:
N/A

What consultation has taken place or is planned with each of the identified groups?
The Policy was developed and approved in consultation with the IG, BI & IM&T Steering Group prior to endorsement by the Integrated Performance and Assurance Committee.

What was the outcome of the consultation undertaken?
Approval and Endorsement sought

What changes or actions do you propose to make or take as a result of research and/or consultation?
Briefly describe the actions then please insert actions to be taken on to the given Improvement Plan template provided. The Information Governance Team on behalf of the Associate Director of Corporate Affairs will be responsible for ensuring that this policy is implemented, including any supporting guidance and training deemed necessary to support the implementation, and for monitoring and providing Governing Body assurance in this respect.

Will the planned changes to the proposal?	**Yes**	**No**
a) Lower the negative impact?	N/A	
b) Ensure that the negative impact is legal under anti-discriminatory law?	N/A	
c) Provide an opportunity to promote equality, equal opportunity and improve relations i.e. a positive impact?	N/A	

Taking into account the views of the groups consulted and the available evidence, please clearly state the risks associated with the proposal, weighed against the benefits.
Information risk - The CCG needs to have safe haven procedures in place to maintain the privacy and confidentiality of any person identifiable information it holds**.**

What monitoring/evaluation/review systems have been put in place?
Monitoring will be undertaken by the Information Governance team. The frequency of review will be every other year or as required.

When will it be reviewed?
July 2023

Date completed:	4th October 2021
Signature:	Information Governance Manager
Approved by:	OD & HR Advisor (Equality and Diversity)
Date approved:	18th October 2021