NHS
Cambridgeshire and
Peterborough
Clinical Commissioning Group

Cambridgeshire and Peterborough Clinical Commissioning Group

REMOVABLE MEDIA POLICY 2021 - 2023

Approval Process

Lead Author(s):	Information Governance Lead / DPO Senior ICT Service Development Manager
Reviewed / Developed by:	Information Governance (IG), Business Intelligence (BI) and IM&T Steering Group members
Approved by:	Information Governance (IG), Business Intelligence (BI) and IM&T Steering Group members – 14th October 2021
Ratified by:	Integrated Performance and Assurance Committee
Date ratified:	23rd November 2021
Version:	5.0
Review date:	October 2023
Valid on:	23rd November 2021

Document Control Sheet

Development and Consultation:	Policy developed in consultation with the Information Governance, Business Intelligence, and IM&T Steering Group.
Dissemination	This policy will be promoted within the CCG and uploaded to the website EMIS Health Support Team to be made aware.
Implementation	The Senior Information Risk Owner is responsible for monitoring the application of the policy by ensuring that: • The policy is brought to the attention of all employees and users of Gemini House. • Members of the Chief Officers Team and Line Managers are aware of their responsibilities for ensuring that staff under their control implement the policy. • Staff are informed and consulted as appropriate. • Any appropriate training and guidance are provided to staff. • Corporate business processes support the implementation of the policy.
Training	Training will be undertaken if required as part of the CCG's ongoing processes.
Audit	Implementation of the Policy will be monitored in line with the data security assurance section of the Data Security and Protection Toolkit (DSPT).
Review	This policy will be reviewed bi-annually or earlier if there are changes in procedures or legislation.
Care Quality Commission	This policy supports the CCG in its compliance with the Care Quality Commission Registration Requirements.
Links with other Policy and Guidance	The Policy should be read in conjunction with: • Information Security for Staff Policy. • Information Governance Policy. • Disciplinary Policy and Procedure.
Equality and Diversity	The OD & HR Advisor (Equality and Diversity) carried out an Equality & Diversity Impact assessment (Annex A) and concluded 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
1.0		Adaptation from NHS Cambridgeshire policy into CCG Policy	April 2013
1.1	Links with other Policy and Guidance	Updated list of policies.	Nov 2013
2.0	Whole document	Reviewed and ratified by CMET.	July 2015
3.0	Whole document	Bi-annual review and update.	April 2017
4.0	Whole document	Bi-annual review and update. Role updated within 3.5. Reference to removable media no longer issued/used within the CCG removed.	November 2019
5.0	Whole document	Bi-annual review and update. Changes in governance arrangements made, changes to building details, and reference to removable media issued / used within the CCG removed	14 October 2021

Table of Contents

1. Introduction

1.1. All staff working in the NHS have a personal responsibility to keep patient identifiable data, personal confidential data, and business sensitive information secure and confidential.

1.2. Recent security incidents across the NHS have highlighted several important issues to bear in mind when transferring such information, particularly in electronic format for example:

- Does the recipient have the right to access the information?
- Does the recipient need to see all the information - can it be anonymised?
- Is the recipient clearly identified and do they know that the information is being transferred to them?
- Is the information encrypted, secure or securely packaged when in transit?
- Are arrangements in place for a confirmation of receipt to be sent?

1.3. This policy aims to prevent unauthorised disclosure, modification, removal or destruction of CCG information assets, and disruption to business activities.

1.4. Under the powers granted to the Information Commissioner's Office since May 2018 a financial penalty of up to the sterling equivalent of 10 million Euros can be raised against an individual or organisation that does not comply with information security requirements and loses personal identifiable data.

1.5. While it is very rare that removable media such as encrypted memory sticks USB) or CD or DVD will be used for the transfer of data such a situation may occur. It is expected that staff wishing to transfer data will have undertaken a Data Protection Impact Assessment (DPIA) and that in most cases transfer will be undertaken using other methods. This policy should be adhered to for all types of data used on removable media regardless of whether the data contained is Patient Identifiable Data or Personal Confidential Data. This ensures that if the removable media is lost or stolen no information governance or security breaches could occur.

1.6. Staff will not use unapproved removable media in any form with any CCG system or hardware.

2. Scope

2.1 Removable media refers to computer storage devices that are not fixed inside a computer and include:

- Tapes
- Removable or external hard disk drives
- Optical disks i.e., DVD and CD
- Solid state memory devices including memory cards, pen drives, memory sticks (USB) etc.
- SD cards

2.2 All removable media for use on information systems owned or operated by the CCG are covered by this procedure.

2.3 Only CCG provided encrypted USB memory sticks are to be used by staff independently. Other removable media are only used with agreement and in conjunction with CCG ICT staff. The use of encrypted USB is being phased out and as such use is increasingly unusual.

3. Responsibilities

3.1 Staff and contractors are not permitted to introduce or use any removable media other than those provided, or explicitly approved for use, by the Senior ICT Service Development Manager on behalf of the CCG.

3.2 Any bulk data extracts (over 50 records) of patient identifiable data or personal confidential data or business sensitive information must be authorised by the responsible member of the Chief Officer Team (COT) for the work area and a log/register kept of such transactions (*see Appendix 1*).

3.3 The Senior ICT Service Development Manager is responsible for ensuring that the CCG has adequate supplies of all removable media that has been approved for use.

3.4 The Senior ICT Service Development Manager is responsible for identifying and arranging the implementation of any device configuration requirements that the CCG may need. This will enable compliance with NHS Information Governance standards and IT security policy and procedures, for example, the restriction of write permission to hard drives, USB port restrictions etc.

3.5 Members of the CCG's Chief Officer Team (COT):

- are responsible for authorising the use of removable media by staff and must record the authorisation in the format outlined in Appendix 1.
- should assure themselves that there is a real business requirement to use removable media.
- in collaboration with the Senior ICT Service Development Manager, are responsible for the day-to-day management and oversight of removable media used within their work areas, to ensure this policy is followed.
- are responsible for the secure storage of all unallocated or returned removable media and any related control documentation required by this procedure.
- are responsible for ensuring that staff authorised to use removable media receive appropriate Information Governance training.

3.6 Staff who have been authorised to use removable media for the purposes of their job roles are responsible for the secure use of those removable media as required by this policy. Failure to comply with this removable media policy may endanger the information services of the CCG and may result in disciplinary or criminal action.

3.7 Staff must not use removable media to store the primary record. The primary record must always be stored on a system authorised for its storage e.g. Adam, Staff ID photographs

3.8 Staff must keep a record of the data that is stored on removable media. In the case of media lost or stolen a copy of this record must be included in the incident report.

3.9 Staff must be aware of policy and procedure governing the work area, including consequences of breach of policy.

3.10 Staff have a responsibility to ensure all individuals with which they work do not use non-approved removable media when working on NHS related activities.

4. Security Procedures

4.1 Removable media shall only be used by staff and contractors who have an identified and agreed business need for them.

4.2 The use of removable media by sub-contractors or temporary workers must be subject to the same risk assessment and authorisation process. (*See Appendix 2*)

4.3 Removable media that have been approved for use within the CCG are to be identified by the Senior ICT Service Development Manager.

4.4 Removable media may only be used to store and share NHS information that is required for a specific business purpose.

4.5 Where patient identifiable data or personal confidential data or business sensitive information is being sent or received, a process must be in place to record the safe receipt.

Note: Only very limited and controlled use of patient identifiable data (PID) / Personal Confidential Data (PCD) is allowed within the CCG. For any processing of PID / PCD under the General Data Protection Regulations a legal basis to do so must be identified. The CCG has very few approved reasons for the use of PID/PCD. Data sharing that includes the use of PID or PCD requires the completion and approval of a Data Protection Impact Assessment (DPIA)

4.6 Data archives or back-ups taken and stored on removable media, either short-term or long-term must take account of any manufacturer’s specification or guarantee.

4.7 Spot check audits and questionnaires will be conducted by the CCG to ensure this policy is complied with. Any compliance issues will be reported to the member of the Chief Officers Team concerned and may be handled through staff disciplinary processes or contractual arrangements.

4.8 All incidents involving the use of removable media must be reported to the Senior ICT Service Development Manager and Information Governance Lead immediately and in accordance with the CCG’s Incident and near miss reporting guidance.

4.9 Removable media should not be taken or sent off-site unless a prior agreement or instruction exists. A record must be maintained of all removable media taken or sent off-site or brought into or received by the organisation. This record should also identify the data files involved. (*See Appendix 1*).

4.10 Removable media must be physically protected against their loss, damage, abuse, or misuse when used, where stored and in transit.

4.11 When the business purpose has been satisfied, the contents of removable media must be removed from that media through a destruction method that makes recovery of the data impossible. Alternatively, the removable media and its data should be destroyed and disposed of beyond its potential reuse. In all cases, a record of the action to remove data from or to destroy data should be recorded in an auditable log file.

5. Unacceptable Use

5.1 The following activities are, in general, prohibited. The list below is by no means exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use.

- The unauthorised storage of patient identifiable data or personal confidential data or business sensitive information on any form of removable media (including memory pens, generic MP3 players, digital cameras, Smartphones etc).

- The connection any removable media, such as digital cameras, generic MP3 players, external hard drives, USB memory sticks etc to the CCG network without prior authorisation from the Senior ICT Service Development Manager.

- Attempting to install applications / or programs from removable media onto any CCG computer assets.

- The saving of non-operational documents, files, or folders from any removable media to any CCG system or hardware.

- Use of USB drives or other mechanisms to subvert Cambridgeshire and Peterborough CCG security controls is expressly forbidden. Any failure to comply with this requirement will be reported to the member of the Chief Officer Team concerned and may be handled through staff disciplinary processes or contractual arrangements.

Appendix 1 – Removable Media Authorisation Request Form

NHS
Cambridgeshire and
Peterborough
Clinical Commissioning Group

AUTHORISATION REQUEST FORM FOR THE USE OF REMOVABLE MEDIA
(Note: Only one application per form)

Name of User (Block Capitals): ____

Job Title: ______________________________ Base: ______________________

Contact Number: ______________________ Date:________________________

I request authorisation to use the following removable media (please tick):

Media Type		**Asset No/ Serial No** *(if approved)*	**Media Type**		**Asset No/ Serial No** *(if approved)*
USB Pen drive			External Hard drive		
CD/DVD			ZIP/DAT drive		
Memory Card					

Other (please specify): ………………………………………………………………………….

The removable media will be used for the following purposes:

PC Asset No. *(If applicable)*	Specific details of data to be transferred	Purpose/Location

I have read and agree to abide by the CCG's Removable Media Policy and Information Security for Staff Policy.

I understand that any breach will result in my access being terminated and may lead to disciplinary action being taken by the CCG.

The issued USB memory key remains the property of the CCG and must be returned to the ICT Department when leaving the organisation or when it is no longer required to fulfil the job role.

Failure to do so will incur a replacement charge for the Unit. This is a nominal £10 for a 1GB USB Stick.

Signature of User……………………………………………… Date: ……………………….
(Cambridgeshire and Peterborough CCG retain ownership of any data that is held on removable media issued)

AUTHORISATION by a member of the CCG Senior Leadership Team (SLT)
I authorise the purchase of the above removable media for the use specified.

I confirm that I understand my responsibility for the day to day management and oversight of this device in accordance with the Removable Media and Information Security for Staff Policies.

Signed: ....

Name (Block capitals): ....

Job Title:.. Date:..

Base: .... Contact no: ....

AUTHORISED/REJECTED BY SENIOR ICT SERVICE DEVELOPMENT MANAGER

Date: ________________________

Authorised (Yes/No) ____________

If no, reason for rejection: ....

....

Signed: ....

Name (Block capitals): ....

ISSUE/RETURN

Date of issue: __________________

Signed (Senior ICT Service Development Manager / Member of the SLT)

....

Name (Block capitals)..

Signed (Member of staff for receipt) ....

Name (Block capitals)..

Date of return: _____________

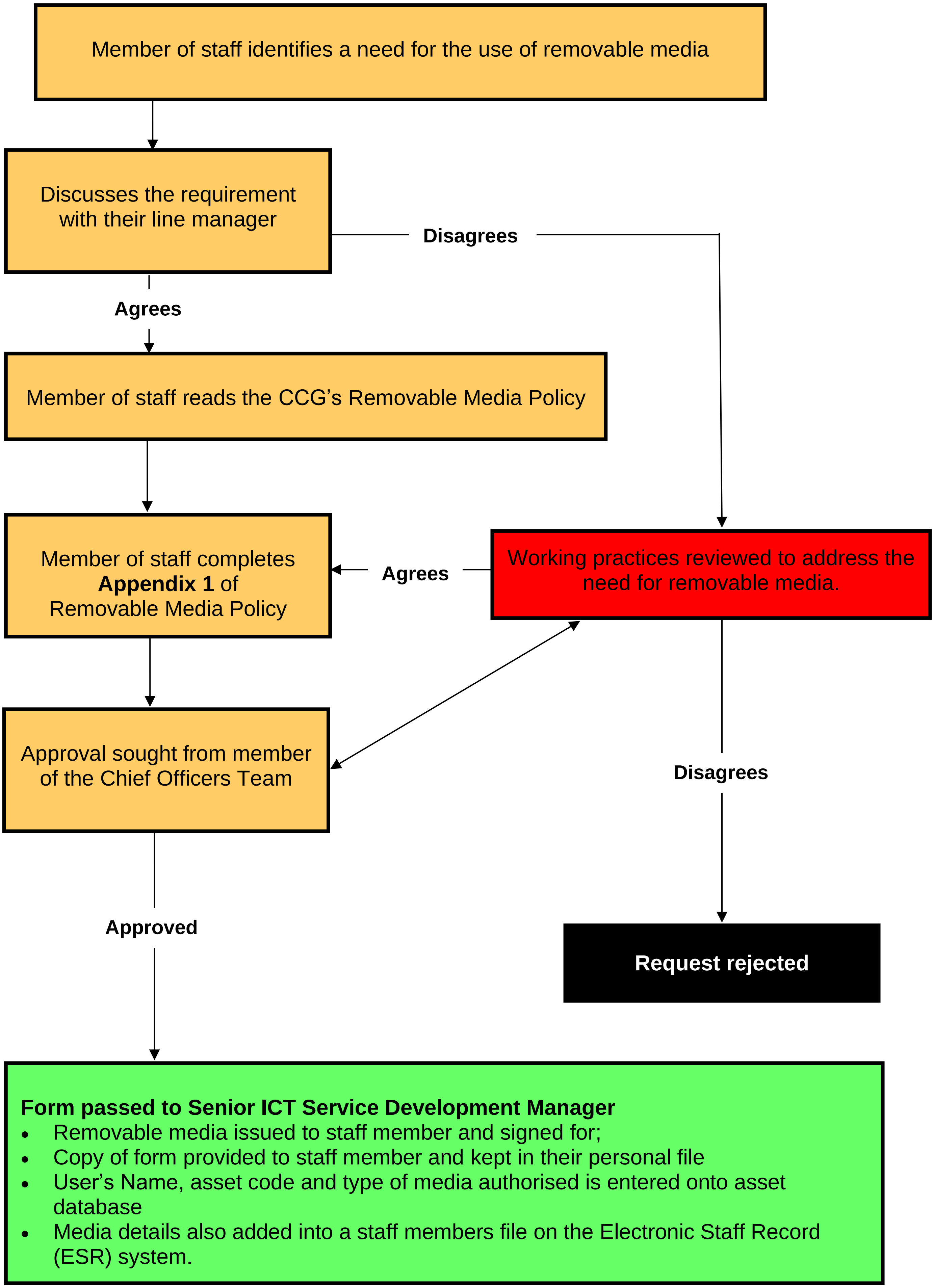
Signed (Senior ICT Service Development Manager / Member of the SLT)

....

Name (Block capitals)..

Signed (Member of staff for return) ....

Appendix 2 - Process for Requesting Removable Media



Member of staff identifies a need for the use of removable media

Discusses the requirement with their line manager

Member of staff reads the CCG's Removable Media Policy

Member of staff completes **Appendix 1** of Removable Media Policy

Working practices reviewed to address the need for removable media.

Approval sought from member of the Chief Officers Team

Request rejected

Form passed to Senior ICT Service Development Manager

- Removable media issued to staff member and signed for;
- Copy of form provided to staff member and kept in their personal file
- User's Name, asset code and type of media authorised is entered onto asset database
- Media details also added into a staff members file on the Electronic Staff Record (ESR) system.

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 Removable Media 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 staff working in the NHS have a personal responsibility to keep patient identifiable data and personal confidential data and business sensitive information secure and confidential. This policy aims to prevent unauthorised disclosure, modification, removal or destruction of CCG information assets, and disruption to business activities.
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 staff newsletter.
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 - This policy aims to mitigate the risk by guiding staff in the prevention of unauthorised disclosure, modification, removal or destruction of CCG information assets, and disruption to business activities.

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?
October 2023

Date completed:	6th October 2021
Signature:	Senior ICT Service Development Manager
Approved by:	OD & HR Advisor (Equality and Diversity)
Date approved:	20th October 2021