CONFIDENTIALITY: CODE OF CONDUCT POLICY

September 2019

Important: This document can only be considered valid when viewed on the CCG's website.

If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.

If you need this document in a different format or language (e.g. large print, Braille, audio or easy read), please contact us on 01482 344700, or email HULLCCG.contactus@nhs.net, or write to: NHS Hull Clinical Commissioning Group, 2nd Floor, Wilberforce Court, Alfred Gelder Street, Hull HU1 1UY.

Name of Policy:	Confidentiality: Code of Conduct Policy
Date Issued:	November 2019
Date to be reviewed:	2 years from approval date

Policy Title:	Confidentiality: Code of Conduct Policy	
Supersedes: (Please List)	All previous Confidentiality:- code of conduct policies	
Description of Amendment(s):	Removal of reference to DPA 98. Updates to password guidance. Updates to policy guidance. Updates to Confidentiality Dos & Don'ts.	
This policy will impact on:	All Staff	
Policy Area:	Data Protection	
Version No:	2.0	
Author:	Information Governance Team	
Effective Date:	November 2019	
Review Date:	September 2021	
Equality Impact Assessment Date:	September 2019	
APPROVAL RECORD	Integrated Audit and Governance Committee	November 2019
Consultation:		
	Members of Senior Leadership Team / Information Governance Steering Group Members / Heads of Teams	October 2019

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Website
0.1	Barry Jackson	First draft for comments	NR	N/A
1.0	Barry Jackson	Approved version	N/A	N/A
1.1	Helen Sanderson	Amendments to reflect HSCIC Guidance and Caldicott 2	N/A	N/A
1.2	Mark Culling	Amendments to reflect the Data Protection Act 1998 (expected to be superseded by a Data Protection Act 2017 incorporating the requirements of the General Data Protection Regulation).		
2.0	Hayley Gillingwater	Removal of reference to DPA 98 Updates to password guidance. Updates to policy guidance. Updates to Confidentiality Dos & Don'ts. Information on the National Opt-Out	Integrated Audit and Governance Committee	November 2019

Contents

1 INTRODUCTION AND APPLICABILITY

The purpose of this Code of Conduct is to lay down the key principles that staff should follow when handling personal confidential/sensitive or corporately sensitive information. All staff should to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

All employees working in the NHS are bound by a legal duty of confidence to protect personal confidential information they may come into contact with during the course of their work. This is not just a requirement under their contractual responsibilities but also a requirement within the common law duty of confidence, the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). This requirement continues to exist after employment has terminated. It is also a requirement within the NHS Care Record Guarantee, produced to assure patients regarding the use of their information.

It is important that staff protect personal confidential/sensitive and corporately sensitive information at all times, and must therefore ensure that they are aware of and comply with all information governance policies and complete their statutory and mandatory information governance training.

2 ENGAGEMENT

This policy has been developed based on the knowledge and experience of the Information Governance team. It is derived from a number of national codes and policies which are considered as best practice and have been used across many public sector organisations.

3 IMPACT ANALYSES

3.1 Equality

This Policy forms part of the CCG's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

As part of its development this Policy and its impact on equality has been analysed and no detriment identified.

4 SCOPE

This policy applies to all staff, CCG Members, temporary staff, seconded staff, contractors and others undertaking work on behalf of the CCG.

5 POLICY PURPOSE AND AIMS

5.1 Confidentiality Principles

All staff must ensure that the following principles are adhered to:-

- Personal confidential information and corporately confidential information must be effectively protected against improper disclosure when it is received, collected, created, stored, transmitted or disposed of.

- Access to personal confidential information or corporately confidential information must be allocated on a need-to-know basis.

- Disclosure of personal confidential information or corporately confidential information must be limited to that purpose for which the disclosure is required.

- Recipients of disclosed information must respect that it is given to them in confidence and treat it accordingly.

- If the decision is taken to disclose information, that decision must be justified and documented.

- Where services which need to regularly or routinely share confidential information in order to provide the service must have an information sharing agreement in place, including service user information leaflets and a process to obtain consent for sharing.

- Any concerns about disclosure must be discussed with either your Line Manager or the Information Governance Team.

5.2 Protecting Personal Confidential and Corporately Sensitive Information

1 The CCG is responsible for protecting all the information it holds at all times and must always be able to justify any decision to share information.

2 Personal confidential information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of data. Appropriate data processing agreements need to be in place to obtain information from the relevant organisations.

3 Access to rooms and offices where terminals are present or personal confidential information or corporately confidential information is stored must be controlled. Doors must be locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place to prevent oversight of personal confidential information or corporately confidential information by unauthorised parties.

4 All staff should clear their desks at the end of each day. In particular they must keep all records containing personal confidential information or corporately confidential information in recognised filing and storage places that are locked.

5 All staff should lock their computer or laptop when away from their desk (activated by ⊞+L or Ctrl+Alt+Del, lock computer)

6 Unwanted printouts containing personal confidential information or corporately confidential information must be put into a confidential waste bin. Discs, tapes, printouts and messages must not be left lying around but be filed and locked away when not in use.

7 Your Contract of Employment includes a commitment to confidentiality. Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

5.3 Disclosing Confidential Information

1. To ensure that information is only shared with the appropriate people and in appropriate circumstances, care must be taken to check those people have a legal basis for access to the information before releasing it.

2. It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

3. Information can be disclosed:

- When effectively anonymised.
- When the information is required by law or under a court order. In this situation staff must discuss with their Line Manager and obtain approval of the Caldicott Guardian.
- In identifiable form, when it is required for a specific purpose, with the individual's written consent or with support under the Health Service (Control of patient information) regulations 2002, obtained via application to the Confidentiality Advisory Group (CAG) within the Health Research Authority1.
- In Vulnerable Adults and Child Protection proceedings if it is considered that the information required is in the public or child's interest. In this situation staff must discuss with their Line Manager and obtain approval of the Caldicott Guardian.
- Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation staff must discuss with their Line Manager and obtain approval of the Caldicott Guardian.

4. If staff have any concerns about disclosing information they must discuss this with their Line Manager or the Information Governance Team.

5. The national data opt-out is a service that allows patients to opt out of their confidential patient information being used for research and planning. Before you disclose any personal information you must ensure that you have taken into account whether the national data opt-out is applicable. It is not applicable for direct care or for the use of anonymised data. More information can be found at the link below or from your IG lead.

https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out

6. Care must be taken in transferring information to ensure that the method used is as secure as it can be. In most instances a Data Sharing, Data Re-Use or Data Transfer Agreement will have been completed before any information is transferred. The Agreement will set out any conditions for use and identify the mode of transfer. For further information on Data Sharing Agreements contact the Information Governance team or see the Information Sharing Protocol.

7. Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mails and surface mail.

8. Transferring patient information by email to anyone outside the CCG network may only be undertaken through the NHS Mail system (i.e. from one NHSnet account to another NHSnet account or to a secure government domain e.g. gov.uk), since this ensures that mandatory government standards on encryption are met. As per the Safe Haven and Email Policies.

Sending information via email to patients is permissible, provided the risks of using unencrypted email have been explained to them, they have given their consent and the information is not person-identifiable or confidential information.

Staff should be made aware of the NHS Mail facility that allows personal confidential information to be sent securely to non- NHS Mail addresses and allows the recipient to respond in a secure manner if necessary. This should be used wherever possible when corresponding with none NHS Mail account holders where confidential information needs to be sent.

5.4 Working Away from the Office Environment

1. There will be times when staff may need to work from another location or whilst travelling. This means that these staff may need to carry CCG information with them which could be confidential in nature e.g. on a laptop, USB stick or paper documents, therefore appropriate measures must be taken to protect the information whilst away from organisational premises.

2. Taking home/ removing paper documents that contain personal confidential information or corporately confidential information from CCG premises must only be done by authorised staff and the minimum information taken. Appropriate security measures must be adopted to protect that information whilst away from organisational premises.

3. 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 current NHS Encryption Guidance.

4. To ensure safety of personal confidential information or corporately confidential information staff must take reasonable steps to ensure the security of that information whilst travelling and ensure that it is kept in a secure place if they take it home or to

another location. Personal confidential information or corporately confidential information must be safeguarded at all times and kept in lockable locations.

5. Staff must minimise the amount of personal confidential information or corporately confidential information that is taken away from CCG premises.

6. If staff do need to carry personal confidential information or corporately confidential information they must ensure the following:

• Any personal confidential information or corporately confidential information must be transported securely. Prior to taking any information out, staff should consider and remember that they may be personally liable for breaches of the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and their Contract of Employment.

7. If staff do need to take personal confidential information or corporately confidential information home they have personal responsibility to ensure the information is 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 information.

8. When you remove equipment and data from NHS premises you are responsible for ensuring its safe transportation and storage as far as is reasonably practical. Computer equipment should be kept out of sight and not be left unattended were possible and when stored in the home, windows and doors should be secured when your home is unoccupied. Computer equipment must be transported in a secure, clean environment and must not be left in a vehicle overnight. You may be held liable if you do not take reasonable precautions.

9. Staff must NOT forward any personal confidential information or corporately confidential information via email to their home e-mail account. Staff must not use or store personal confidential information or corporately confidential information on a privately owned computer or device.

5.5 Carelessness

1. All staff have a legal duty of confidence to keep personal confidential information or corporately confidential information private and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must not:

- Talk about personal confidential information or corporately confidential information in public places or where they can be overheard.
- Leave any personal confidential information or corporately confidential information lying around unattended, this includes telephone messages, computer printouts, and other documents, and
- Leave a computer terminal logged on to a system where personal confidential information or corporately confidential information can be accessed, unattended.

2. Steps must be taken to ensure physical safety and security of personal confidential information or corporately confidential information held in paper format and on computers.

3. Passwords must be kept secure and must not be disclosed any other person. Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. This is a disciplinary offence and constitutes gross misconduct which may result in summary dismissal.

- Passwords should not be written down.
- Passwords should not relate to the employee or the system being accessed.
- Passwords MUST be changed from default values and should not be easy to guess.
- Passwords should not be shared with colleagues.
- Passwords should not be reused; staff should use a different password for each system.

5.6 Abuse of Privilege

1 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 a breach of confidentiality, the Data Protection Act 2018 and the General Data Protection Regulation.

2 When dealing with personal confidential information or corporately confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of CCG.

3 If staff have concerns about this issue they should discuss it with their Line Manager or Information Governance Team.

5.7 Confidentiality Audits

Good practice requires that all organisations that handle person confidential or confidential information put in place processes to highlight actual or potential confidentiality breaches in their systems, and also procedures to evaluate the effectiveness of controls within these systems. This function will be co-ordinated by the Policy Directorate Information Governance team through a programme of audits.

6 IMPLEMENTATION

The policy will be disseminated by being made available on the NHS Hull CCG website and highlighted to staff through newsletters, team briefings and by managers.

'Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCG's disciplinary procedure'.

7 TRAINING AND AWARENESS

Staff will be made aware of the policy via the website.

8 MONITORING AND AUDIT

Adherence to this policy will be monitored on an on-going basis and breaches may result in disciplinary procedures.

9 POLICY REVIEW

This policy will be reviewed in 2 years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

10 REFERENCE MATERIALS

- NHS Confidentiality Code of Practice
- HSCIC(NHS Digital): Code of Practice on Confidential Information
- HSCIC (NHS Digital): A Guide to Confidentiality in Health and Social Care
- NHS Digital: Encyption Guide for NHS Mail V5.0 May 2019
- Report of the Caldicott2 Review - Information: To share or not to share? The Information Governance Review 2013
- Government Response to Report of the Caldicott2 Review 2013
- National Data Guardian for Health & Care: Review of Data Security, Consent and Opt-Outs
- The Independent Information Governance Oversight Panel: Annual Report

ANNEX A: Confidentiality Dos and Don'ts

Do's

- Do safeguard the confidentiality of all personal confidential information or corporately confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of NHS.

- Do clear your desk at the end of each day, keeping all portable records containing personal confidential information or corporately confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.

- Do switch off computers with access to personal confidential information or corporately confidential information, or put them into a password protected mode, if you leave your desk for any length of time; (activated by ⊞+L or Ctrl+Alt+Del, lock computer).

- Do ensure that you cannot be overheard when discussing confidential matters.

- Do challenge and verify where necessary the identity of any person who is making a request for personal confidential information or corporately confidential information and ensure they have authorisation to access, and a legitimate need to know the information.

- Do share only the minimum information necessary.

- Do transfer personal confidential information or corporately confidential information securely, i.e. use an nhs.net email account to send confidential information to another nhs.net email account or to a secure government domain e.g .gov.uk.

- Do seek advice if you need to share personal confidential information without the consent of the patient/identifiable person's consent, and record the decision and any action taken.

- Do report any actual or suspected breaches of confidentiality at the earliest opportunity.

- Do complete statutory and mandatory training and other training as appropriate.

Don’ts

- Don’t share passwords or smart cards, or leave them lying around for others to see or use.
- Don’t disclose or share information to someone where there is not a legal basis to do so.
- Don’t share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.
- Don’t use personal confidential or corporately confidential information unless absolutely necessary, anonymise the information where possible.
- Don’t collect, hold or process more information than you need, and do not keep it for longer than necessary.
- Don’t attempt to obtain access to personal confidential information or corporately confidential information unless you have a legitimate reason to do so.
- Don’t leave confidential messages on answering machines or text patients without their prior consent.
- Don’t leave computer equipment or records in a vehicle overnight.

Appendix 1

HR / Corporate Policy Equality Impact Analysis:	
Policy / Project / Function:	Code of Confidentiality Policy v1.2
Date of Analysis:	17/01/2018 Reviewed 17/09/2019
Completed by: **(Name and Department)**	Dr Mark Culling Review: Hayley Gillingwater Information Governance Team
What are the aims and intended effects of this policy, project or function?	The purpose of this Code of Conduct is to lay down the key principles that staff should follow when handling personal confidential/sensitive or corporately sensitive information. All staff should to be aware of their responsibilities for safeguarding confidentiality and preserving information security.
Are there any significant changes to previous policy likely to have an impact on staff / other stakeholder groups?	No No changes following policy review.
Please list any other policies **that are related to or referred to as part of this analysis**	The Health and Social Care Act 2012 Caldicott 2 Principles –To Share or Not to Share? Common Law Duty of Confidentiality HSCIC Guide to Confidentiality in Health and Social Care General Data Protection Regulation (GDPR) Data Protection Act 2018

Who will the policy, project or function affect?	Employees and the general public
What engagement / consultation has been done, or is planned for this policy and the equality impact assessment?	Consultation on the new policy has taken place nationally and locally. Consultation on the updated policy has taken place locally.
Promoting Inclusivity and Hull CCG's Equality Objectives. How does the project, service or function contribute towards our aims of eliminating discrimination and promoting equality and diversity within our organisation? How does the policy promote our equality objectives: 1. Ensure patients and public have improved access to information and minimise communications barriers 2. To ensure and provide evidence that equality is consciously considered in all commissioning activities and ownership of this is part of everyone's day-to-day job 3. Recruit and maintain a well-supported, skilled workforce, which is representative of the population we serve 4. Ensure the that NHS Hull Clinical Commissioning Group is welcoming and inclusive to people from all backgrounds and with a range of access needs	The policy does not directly promote inclusivity but provides a framework for the CCG's approach to acceptable computer use within the workplace, ensuring staff are supported by management and health professionals

Equality Data	
Is any Equality Data available relating to the use or implementation of this policy, project or function? Equality data is internal or external information that may indicate how the activity being analysed can affect different groups of people who share the nine *Protected Characteristics* – referred to hereafter as *'Equality Groups'.* Examples of *Equality Data* include: (this list is not definitive) 1: Recruitment data, e.g. applications compared to the population profile, application success rates 2: Complaints by groups who share / represent protected characteristics 4: Grievances or decisions upheld and dismissed by protected characteristic group 5: Insight gained through engagement	Yes ✓ No ☐ Where you have answered yes, please incorporate this data when performing the *Equality Impact Assessment Test* (the next section of this document). If you answered No, what information will you use to assess impact? **Please note that due to the small number of staff employed by the CCG, data with returns small enough to identity individuals cannot be published. However, the data should still be analysed as part of the EIA process, and where it is possible to identify trends or issues, these should be recorded in the EIA.**

Assessing Impact				
Is this policy (or the implementation of this policy) likely to have a particular impact on any of the protected characteristic groups? **(Based on analysis of the data / insights gathered through engagement, or your knowledge of the substance of this policy)**				
Protected Characteristic:	**No Impact:**	**Positive Impact:**	**Negative Impact:**	**Evidence of impact and, if applicable, justification where a *Genuine Determining Reason*[1] exists (see footnote below – seek further advice in this case)**
Gender	X			This policy applies to all regardless of gender
Age	X			This policy applies to all regardless of age
Race / ethnicity / nationality	X			This policy applies to all staff regardless of race/ethnicity. Analysis of employee data indicates that the percentage of white employees is reflective of the local population. However, the proportion of BME staff is lower than that of the local population it serves All staff require

1. [1] *The action is proportionate to the legitimate aims of the organisation (please seek further advice)*

				competencies which include the ability to read and understand English or to request the information in another format available to them
Disability	X			This policy applies to all regardless of disability
Religion or Belief	X			This policy applies to all regardless of religion or belief
Sexual Orientation	X			This policy applies to all, regardless of sexual orientation
Pregnancy and Maternity	X			This policy applies to all regardless of pregnancy or maternity
Transgender / Gender reassignment	X			This policy applies to all regardless of transgender/gender reassignment
Marriage or civil partnership	X			This policy applies to all regardless of marriage or civil partnership

Action Planning:				
As a result of performing this analysis, what actions are proposed to remove or reduce any risks of adverse impact or strengthen the promotion of equality?				
Identified Risk:	**Recommended Actions:**	**Responsible Lead:**	**Completion Date:**	**Review Date:**
Staff should have English Language	The CCGs internal 'portal' and external website	CCG Communications	Updating of this facility is	Next Policy

competencies as part of the essential recruitment criteria. Suggest rewording to: Staff or contractors may have additional communications needs, which need to be supported by the CCG.	signpost individuals to alternative formats such as large print, braille or another language.		ongoing	Review – September 2020

Sign-off
All policy EIAs must be signed off by Mike Napier, Associate Director of Corporate Affairs
I agree with this assessment / action plan
If *disagree*, state action/s required, reasons and details of who is to carry them out with timescales:
 **Signed:**
Date: 09.10.19