NHS
Harrogate and Rural District
Clinical Commissioning Group

Confidentiality: Code of Conduct Policy

November 2017

Authorship:	**Barry Jackson – Information Governance, Security and Compliance Manager**
Committee Approved:	Audit Committee
Approved date:	November 2017
Review Date:	November 2020
Equality Impact Assessment:	Completed
Target Audience:	Council of Members, Governing Body and its Committees and Sub-Committees, CCG Staff, agency and temporary staff & third parties under contract
Policy Number:	056
Version Number:	3.0

The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as 'uncontrolled' and as such may not necessarily contain the latest updates and amendments.

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 Intranet
0.1	Barry Jackson	First draft for comments	NR	
1.0	Barry Jackson	Approved version		
1.1	Helen Sanderson	Amendments to reflect HSCIC Guidance and Caldicott 2	Audit Committee March 2016	
2.0	IG Officer	Caldicott Requirements	Dec 2016	
3.0	IG Officer	• To update for changes in organisational relationships (CSU to Embed) • To update for the requirements of the General Data Protection Regulation	Audit Committee November 2017	January 2018

CONTENTS

		Page
1	**Introduction & Applicability**	4
2	**Engagement**	4
3	**Impact Analyses** **3.1 Equality**	4
4	**Scope**	5
5	**Policy Purpose and Aims**	5 - 8
6	**Implementation**	9
7	**Training and Awareness**	9
8	**Monitoring and Audit**	10
9	**Policy Review**	10
	ANNEX A: Confidentiality Dos and Don'ts	11 - 12
	Appendices – Appendix 1 – Equality Impact Analysis	13

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 current Data Protection Legislation and 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

An equality impact screening analysis has been carried out on this policy and is attached at Appendix 1.

As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

.

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

6 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 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. 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.

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

7. 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. gsi.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 carried in a suitable lockable container, etc. Prior to taking any information out, staff should consider and remember that they may be personally liable for breaches of current Data Protection Legislation 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. 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, faxes 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.

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 and of the current Data Protection Legislation.

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 intranet 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 & AWARENESS

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

8 MONITORING & 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: Code of Practice on Confidential Information
- HSCIC: A Guide to Confidentiality in Health and Social Care
- HSCIC: Sending an encrypted email from NHSmail to a non-secure email address
- 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

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.

- 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. gsi.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.

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

- Obtain and record consent for the use of data subjects personal information

Don’ts

- Don’t share passwords or smart cards, or leave them lying around for others to see or use.

- 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.

Appendix 1

1. Equality Impact Analysis	
Policy / Project / Function:	Confidentiality: Code of Conduct Policy
Date of Analysis:	13/01/14
This Equality Impact Analysis was completed by: **(Name and Department)**	C Wallace - IG Manager – CSU IG 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.
Please list any other policies that are related to or referred to as part of this analysis?	
Who does the policy, project or function affect ? Please Tick ✔	Employees ☒ Service Users ☐ Members of the Public ☐ Other (List Below) ☐

2. **Equality Impact Analysis: Screening**					
	Could this policy have a positive impact on…		Could this policy have a negative impact on…		Is there any evidence which already exists from previous (e.g. from previous engagement) to evidence this impact
	Yes	No	Yes	No	
Race	☐	☒	☐	☒	
Age	☐	☒	☐	☒	
Sexual Orientation	☐	☒	☐	☒	
Disabled People	☐	☒	☐	☒	
Gender	☐	☒	☐	☒	
Transgender People	☐	☒	☐	☒	
Pregnancy and Maternity	☐	☒	☐	☒	
Marital Status	☐	☒	☐	☒	
Religion and Belief	☐	☒	☐	☒	
Reasoning					
If there is no positive or negative impact on any of the Nine Protected Characteristics go to Section 7					