CR07 - Confidentiality Policy and Procedure

Category: Care Management **Sub-category:** Rights & Abuse

Policy Review Sheet

Review Date: 16/01/17 **Policy Last Amended:** 16/01/17

Next planned review in 12 months, or sooner as required.

Note: The full policy change history is available in your online management system.

Business Impact:	Low	Medium	High	Critical
		X		
Changes are important, but urgent implementation is not required, incorporate into your existing workflow.				

Reason for this review:	Scheduled review
Were changes made?	Yes
Summary:	Converted to new format. Updated to reflect Caldicott Requirements and Guide to Confidentiality in Health and Social Care.
Relevant Legislation:	• The Health and Social Care (Safety and Quality) Act 2015 • The Care Act 2014 • Data Protection Act 1998 • Freedom of Information Act 2000 • Human Rights Act 1998
Underpinning Knowledge - What have we used to ensure that the policy is current:	• HM Government, (2015), *Information sharing Advice for practitioners providing safeguarding services to children, young people, parents and carers*. [Online] Available from: https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice [Accessed: 21/12/2016] • Nursing and Midwifery Council, (2015), *The Code - Professional standards of practice and behaviour for nurses and midwives*. [Online] Available from: https://www.nmc.org.uk/globalassets/sitedocuments/nmc-publications/nmc-code.pdf [Accessed: 22/12/2016] • Royal College of Nursing, (2012), *Nursing staff using personal mobile phones for work purposes- RCN Guidance*. [Online] Available from: https://www2.rcn.org.uk/__data/assets/pdf_file/0009/472464/004259.pdf [Accessed: 03/01/2017] • Department for Constitutional Affairs, (2007), *The Mental Capacity Act Code of Practice*. [Online] Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/497253/Mental-capacity-act-code-of-practice.pdf [Accessed: 03/01/2017]

CR07 - Confidentiality Policy and Procedure

Suggested action:	- Notify all staff of changes to policy - Share key facts with people involved in the service - Training sessions - Discuss in team meetings - Discuss in supervision sessions - Confirm relevant staff understand the content of the policy

CR07 - Confidentiality Policy and Procedure

1. Purpose

1.1 Service Users, their families and staff have a right to believe, and expect, that private and personal information given in confidence will only be used for the purposes for which it was originally given, and not released to others without their consent. The purpose of this policy and procedure is to:

- Ensure that sensitive information is only shared for the purpose of a Service User's wellbeing such as ensuring person-centred care or treatment or protecting the person from abuse
- Ensure that all information is collected, recorded, stored, shared and disposed of in the best interests of the Service User and staff with regard for their human rights and in line with legislation
- Ensure the Service User and staff are aware of the organisation's confidentiality policy and procedure
- Ensure any staff employed or engaged by will be expected to comply with this policy and procedure

1.2 To support in meeting the following Key Lines of Enquiry:

Key Question	Key Line of Enquiry (KLOE)
SAFE	S2: How are risks to individuals and the service managed so that people are protected and their freedom is supported and respected?
WELL-LED	W2: How does the service demonstrate good management and leadership?

1.3 To meet the legal requirements of the regulated activities that is registered to provide:

- The Health and Social Care (Safety and Quality) Act 2015
- The Care Act 2014
- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998

2. Scope

2.1 The following roles may be affected by this policy:

- All staff

2.2 The following Service Users may be affected by this policy:

- All service users

2.3 The following stakeholders may be affected by this policy:

- Family
- Advocates
- Commissioners
- External health professionals
- Local Authority
- NHS

CR07 - Confidentiality Policy and Procedure

3. Objectives

3.1 To outline the principles related to confidentiality and to support staff in applying these principles.

3.2 To establish 's approach to ensuring the confidentiality of personally identifiable information.

3.3 To inform Service User's, their families, stakeholders and carers about 's confidentiality obligations and how we intend to meet them.

3.4 Inform staff working for, or on behalf of, of their responsibilities with regards to confidentiality and personally identifiable information and how will enable these to be met.

4. Policy

4.1 recognise that we have a duty of confidentiality to its Service User and staff. We believe that respecting an individuals' right to a private life which includes confidentiality is important in ensuring a trusting, caring environment where both Service Users and staff are confident that information about them will be protected safely and not shared inappropriately or unnecessarily.

It is the policy of that we will only share information that is in the best interest of the Service User and, with their consent. We aim to comply with the relevant legislation, including the 7 Caldicott principles and Health and Social Care Information Centre (2013) 5 Rules on Confidentiality.

4.2 It is therefore our policy that:

- We will share with people, their families and their carers, as far as the law allows, the information they want or need to know about their health, care and ongoing treatment sensitively and in a way they can understand
- Confidential information will not be used for a different purpose or passed on to anyone else without the consent of the information provider
- There may be occasions when it could be detrimental to the Service User or to another individual if this principle is strictly adhered to
- That there is a recognition breaches of confidence are often unintentional. They are often caused by staff conversations being overheard, by files being left unattended, or by poor computer security. However, the consequences could be equally serious for all concerned
- will ensure that personally identifiable information will always be held securely and, when used, treated with respect. This rule will apply whether the information is held manually or on a computer, on video or audiotape or in a member of staff's head
- We respect that a person's right to privacy and confidentiality continues after they have died
- All information regarding the people we support will be treated with respect and integrity
- In general, no information may be disclosed either verbally or in writing to other persons without the Service User consent. This includes family, friends and private carers, and other professionals
- If in doubt, staff will consult the Line Manager or Ms Tracey Klue Tracey@wellbeingcaregroup.com 01775760563
- Conversations relating to confidential matters affecting Service User should not take place anywhere they may be overheard by others, i.e. in public places - such as supermarkets, corridors or communal areas, etc.
- Written records and correspondence must be kept securely at all times when not being used by a member of staff. Timesheets, rotas, etc. must not be left in unattended vehicles
- Staff will not disclose any information that is confidential or that, if it were made public, may lead to a breakdown in the trust and confidence that the Service User and their families have in
- Staff will not pass on any information, or make comment, to the press or other media. Media enquiries should be referred the person responsible for handling any media enquiries

4.3 All clinical staff are bound by their professional code of ethics issued by their relevant licensing body, such as the General Medical Council, The Nursing and Midwifery Council and the Royal Pharmaceutical Society.

4.4 Responsibilities - All staff should ensure:

CR07 - Confidentiality Policy and Procedure

- When responsible for confidential information, staff must ensure that the information is **effectively protected** against improper disclosure when it's **received, stored, transmitted and disposed** of
- Confidential information must only be accessed if it is appropriate to the job you undertake
- Every effort must be made to ensure that the Service User understand how information about them will be used before they supply any confidential information
- When Service User's give consent to disclosure of information about them, you must make sure they understand what will be disclosed, the reasons for disclosure and the likely consequence/s
- You must make sure that Service Users understand when information about them is likely to be disclosed to others involved in their care, and that they have the opportunity to withhold permission
- If you are required to disclose information outside the team that could have personal consequences for Service User, you must obtain their consent
- If the Service User withholds consent, or if consent cannot be obtained for whatever reason, disclosures may be made only where:
  - **They can be justified in the public interest (usually where disclosure is essential to protect the Service User or someone else from the risk of significant harm)**
  - **They are required by law or by order of a court**
- If you are required to disclose confidential information you should release only as much information as is necessary for the purpose
- You must make sure that the persons to whom you disclose information understand that it is given to them in confidence which they must respect
- If you decide to disclose confidential information, you must be prepared to explain and justify your decision. If you have any doubts discuss them with your line manager
- Any queries concerning the QCS Confidentiality Policy and Procedure should be brought to the attention of your line manager in the first instance
- During their induction period, all staff must be made aware of this policy and their individual responsibilities

4.5 Responsibilities - Registered Manager

- The Registered Manager is responsible for ensuring all workers are advised not to leave documentation in a place where an unauthorised person could gain access to it or discuss people who use our services in a public place
- The Registered Manager is responsible for ensuring all written personal records held concerning individuals are kept securely in a locked cabinet. This excludes the Service User's own copy
- The Registered Manager is responsible for ensuring that any hard copies of individual’s names and addresses or Employees names and addresses that have been generated via the computer, e.g.: problem lists, availability lists, etc, must be destroyed in confidential waste. Under no circumstance may such information be disposed of with household/office rubbish
- The Registered Manager must ensure that all staff understand this policy at the start of employment and its importance is reiterated during supervision or team meetings
- The Registered Manager along with the Registered Provider must ensure that Confidentiality rules are not used as a barrier to sharing appropriate information and fulfilling Duty of Candour obligations

CR07 - Confidentiality Policy and Procedure

5. Procedure

5.1 General Principles of Confidentiality

- Staff should be aware that Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately
- Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared. Seek their agreement unless it is unsafe or inappropriate to do so
- Seek advice if you are in any doubt, without disclosing the identity of the person where possible
- Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgment, that lack of consent can be overridden in the public interest
- Consider safety and well-being: Base your information sharing decisions on considerations of the safety and wellbeing of the person and others who may be affected by their actions
- **Necessary, proportionate, relevant, accurate, timely and secure:** Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely
- Keep a record of your decision and the reasons for it - whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose

5.2 Maintaining Confidentiality

- All information regarding the people we support will be treated with respect and integrity
- In general, no information may be disclosed either verbally or in writing to other persons without the Service User's consent. This includes family, friends and private carers, and other professionals
- If in doubt, you should consult your Line Manager Ms Tracey Klue Tracey@wellbeingcaregroup.com 01775760563
- Conversations relating to confidential matters affecting Service Users should not take place anywhere they may be overheard by passers by, i.e. in public places - such as supermarkets, corridors or communal areas, etc.
- Written records and correspondence must be kept securely at all times when not being used by a member of staff. Timesheets, rotas, etc. must not be left in unattended vehicles
- You must not disclose any information that is confidential or that, if it were made public, may lead to a breakdown in the trust and confidence that the people have in
- You must not pass on any information, or make comment, to the press or other media. Media enquiries should be referred the person responsible for handling any media enquiries

5.3 Safeguarding, The Care Act and Confidentiality

Where safeguarding issues arise and in order to fully understand what has gone wrong, Safeguarding Adult Boards may ask for information to be shared. Decisions about who needs to know and what needs to be known should be taken on a case by case basis, within locally agreed policies and the constraints of the legal framework. However:

- Information will only be shared on a ‘need to know’ basis when it is in the interests of the adult
- Confidentiality must not be confused with secrecy
- Informed consent should be obtained but, if this is not possible and other adults are at risk of abuse or neglect, it may be necessary to override the requirement
- It is inappropriate for to give assurances of absolute confidentiality in cases where there are concerns about abuse, particularly in those situations when other adults may be at risk

5.4 Rights of all Service Users

All Service Users may view personal information we hold about them. Local and Health Authorities are not required to give access to information that is ‘hurtful’ or ‘that would breach the confidentiality of another Service User’. 's policy is to record information in a way that as far as possible avoids a need for this exclusion. If a Service User believes their right to confidentiality is either being breached or undermined, they must have access to 's complaints procedure.

CR07 - Confidentiality Policy and Procedure

5.5 Rights of All Staff

All staff may view personal information held by that relates to them, by applying in writing to their Line Manager, where a member of staff believes that their right to confidentiality is being denied.

5.6 Written Records

- Any record that contains information about an individual should remain confidential unless it is in the public domain. Any records should be factual and should not include the personal opinions of the person writing the records
- Reproduction of information relating to a Service User (for example photocopying documents) should only be done with the consent of the Service User
- Confidential information to be posted must be marked 'Private & Confidential, for attention of the addressee only', and sent recorded/special delivery
- Information held within should not be shown to unauthorised individuals or be left where authorised personnel may access them. All record should be kept in a lockable cabinet in a lockable office, with restricted access
- All written records should be kept securely and only disposed of, by shredding, after appropriate timescales. Staff should take care when recording personal identifiable information into personal note books or paper during shift handover and ensure the safekeeping and destruction of the information.
- Any employee who breaches this policy may be subject to disciplinary procedures

5.7 Telephone - General

Confidential information relating to any individual, either using our services or working within , should not be given to anyone over the telephone except:

- In the case of an emergency, for example, emergency services
- To relatives and/or advocates as appropriate with the Service User consent
- To a professional involved with and known to the individual, for example GP, Social Worker

Where there is any doubt regarding the right of an individual requesting the information, no information should be given, and advice should be sought from the immediate line manager. This includes key safe numbers or access arrangements.

Mobile Phones including Smartphones

Confidentiality must always be respected; not all conversations are appropriate in a public place or in another person’s home.

Staff will be required to comply with 's policy on Mobile phones.

Where smartphones, apps on smart phones or devices are used in the delivery of care, these should be protected with a passcode and the information within them treated as confidential information.

5.8 Social Media

Staff are not permitted to discuss the people who use our services, other employees past or present, or on any social networking site as this may breach confidentiality and bring into disrepute. Staff must also be aware that this applies to taking and posting photographs of Service Users.

5.9 Facsimile

Faxed information is not secure and may be read by anyone in the area at the end source. Confirmation should be sought prior to faxing, that the information being sent would remain confidential to addressee only.

5.10 Verbal

Discussions about a Service User or staff member should not take place if the conversation could be overheard or if there are doubts regarding the confidentiality of the other person. Staff must be aware that individuals not

CR07 - Confidentiality Policy and Procedure

employed by are not bound by the same rules of confidentiality.

It would be considered inappropriate behaviour to make reference to another Service User in conversation with any Service User. Staff must be aware that this applies to discussing other Service Users with each other in front of another Service User.

5.11 Electronic Confidentiality Including CCTV

- will comply with the Data Protection Act and we are aware that if we are processing personal information we may be required to register with Information Commissioner's Office
- Personal data must be obtained lawfully, maintained accurately and securely, and used only for the lawful purposes described in our register entry
- Access to computer files containing personal information is by passwords known to authorised users only
- Employees are required to ensure that computer screens are not left showing personal data in an area where unauthorised people could read it
- Printouts, which contain personal data, should be disposed of securely, for example by shredding
- Service Users and staff may request (in writing) to see the information, which is held about them on computer. All requests for a copy of personal data stored should be made in conjunction with a Senior Manager, if applicable
- Where CCTV is utilised will consider the CQC document on Surveillance

5.12 Mental Capacity and Confidentiality

The Mental Capacity Act 2005 applies to adults without capacity, and further details about the disclosure of confidential information about a Service User lacking capacity can be found in the Mental Capacity Act Code of Practice.

CR07 - Confidentiality Policy and Procedure

6. Definitions

6.1 Data Protection Act 1998 (DPA 98)

- Provides controls on the handling of personal identifiable information for all living individuals
- Central to the Act is compliance with the eight data protection principles, designed to protect the rights of individuals about whom personal data is processed whether an electronic or a paper record

6.2 The Caldicott Report 1997

- Provides guidance to the NHS on the use and protection of personal confidential data (PII), and emphasises the need for controls over the availability of such information and access to it
- It makes a series of recommendations which led to the requirement for all NHS organisations to appoint a Caldicott Guardian who is responsible for compliance with the 6 (original) Caldicott confidentiality principles

6.3 Common Law Duty of Confidentiality

- Prohibits use and disclosure of information, provided in confidence unless there is a statutory requirement or court order to do so
- Such information may be disclosed only for purposes that the subject has been informed about and has consented to, provided also that there are no statutory restrictions on disclosure
- This duty is not absolute, but should only be overridden if the holder of the information can justify disclosure as being in the public interest, for example, to protect the vital interests of the data subjects or another person, or for the prevention or detection of a serious crime

6.4 Safe Haven

- **A Safe Haven** is a term used to explain an agreed set of arrangements that are in place in an organisation to ensure that confidential identifiable information (e.g. patients and staff information) can be communicated safely and securely
- It is a recognised phrase within the NHS but has relevant underlying principles for all community based services

6.5 Personal Information

- **Personal information** is information which can identify a person – in which the person is the focus of the information and which links that individual to details which would be regarded as private. E.g. name and private address, name and home telephone number, etc.

6.6 Sensitive Personal Information

- **Sensitive personal information** is where the personal information contains details of that person's:
  - Health or physical condition
  - Sexual life
  - Ethnic origin
  - Religious beliefs
  - Political views
  - Criminal convictions

6.7 Business Sensitive information.

- **I**nformation that if disclosed could harm or damage the reputation or image of an organisation

CR07 - Confidentiality Policy and Procedure

6.8 Public Interest

- Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest
- Decisions about the **public interest** are complex and must take account of both the potential harm that disclosure may cause and the interest of society in the continued provision of confidential services
- The Public Interest Disclosure Act (Whistleblowing) has more information about this

6.9 Consistent Identifier

- The Health and Social Care (Safety and Quality) Act 2015 includes a requirement for health and adult social care organisations to use a **consistent identifier** (the NHS Number) for all data sharing associated with or facilitating care for an individual
- The NHS Number is the national, unique **identifier** that makes it possible to share patient and Service User information across the NHS and social care safely, efficiently and accurately

6.10 Confidentiality

- Confidentiality means that professionals should not tell other people personal things about a Service User unless the Service User says they can, or if it is absolutely necessary

6.11 Statutory Duty to Disclose

- There are Acts of Parliament which require the production of confidential information
  - Prevention of Terrorism Acts
  - Road Traffic Act
  - Public Health Acts
  - Police and Criminal Evidence Act 1984
  - Misuse of Drugs Act 1971
- It is essential that there is good justification to disclose confidential information when relying upon an Act of Parliament. Public Health legislation requires the reporting of notifiable diseases

Key Facts - Professionals

Professionals providing this service should be aware of the following:

- Professionals can only tell other people your personal information if the Service User says they can or if they have to
- Professionals can share information without a Service Users consent if there is a risk of serious harm to a Service User or other or there is a risk of a serious crime
- When someone dies, confidentiality still applies
- Necessary, proportionate, relevant, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely

CR07 - Confidentiality Policy and Procedure

Key Facts - People affected by the service

People affected by this service should be aware of the following:

- Every person has a right to confidentiality, however, staff may have to share information about you in your best interests
- Where possible, staff will obtain your consent to share information about you
- If you are unable to consent to share information because you lack mental capacity, staff will need to follow the Mental Capacity Act Code of Practice

Further Reading

As well as the information in the 'underpinning knowledge' section of the review sheet we recommend that you add to your understanding in this policy area by considering the following materials:

- **Health and Social Care Information Centre - A Guide to Confidentiality in Health and Social Care** v1.1 September 2013 http://content.digital.nhs.uk/media/12822/Guide-to-confidentiality-in-health-and-social-care/pdf/HSCIC-guide-to-confidentiality.pdf
- **Information: To Share or not to Share - The Information Governance Review.** - March 2013 Fiona Caldicott - Department of Health https://www.gov.uk/government/publications/the-information-governance-review
- **Using surveillance Information for providers of health and social care on using surveillance to monitor services** December 2014 (updated with new regulations in June 2015): **Care Quality Commission** https://www.cqc.org.uk/sites/default/files/20150617_provider_surveillance_information.pdf

Related Policies

- CCTV Policy and Procedure
- Professional Relationships Policy and Procedure
- Obtaining Medical Reports Policy and Procedure
- Access to Information Policy and Procedure
- Data Security Breach Policy and Procedure
- Employee Handbook
- Whistleblowing Policy and Procedure
- Social Networking Policy and Procedure
- Child Protection Policy and Procedure
- Safeguarding Policy and Procedure

Outstanding Practice

To be outstanding in this policy area you could provide evidence that:

- Staff treat Service Users with kindness and respect, and maintain Service User and information confidentiality
- Each person's privacy needs and expectations should be identified, recorded, and met as far as is reasonably possible
- Staff are registered as Dignity Champions and can evidence they follow the 'Dignity Dos'
- Robust systems and Governance process ensure staff and Service User confidentiality is maintained at all times

CR07 - Confidentiality Policy and Procedure

This page is deliberately left blank