Next Steps Mental Healthcare LTD
32 Kingscliffe Street Moston Manchester Lancashire M9 4PG

Review Sheet

Last Reviewed 23 Jun 2025

Last Amended 23 Jun 2025

This policy will be reviewed as needs require or at the following interval: Annual

Business Impact:	LOW — Minimal action required. Circulate information amongst relevant parties.
Reason for this Review:	Scheduled review
Changes Made:	Yes
Summary:	This policy details the rights of Service User / Residents in relation to confidentiality, UK GDPR, data protection and the issues that staff need to be aware of. It has been reviewed with some minor word changes. The Underpinning Knowledge and Further Reading references have also been reviewed and updated to ensure they remain current.
Relevant Legislation:	• The Care Act 2014 • Freedom of Information Act 2000 • Human Rights Act 1998 • Data Protection Act 2018 • UK GDPR • The Health and Social Care (Safety and Quality) Act 2015
Underpinning Knowledge:	• Author: GOV UK, (2024), Information sharing advice for safeguarding practitioners - Guidance on information sharing for people who provide safeguarding services to children, young people, parents and carers [Online] Available from: https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice [Accessed: 23/06/2025] • Author: National Data Guardian, (2021), Guidance about the appointment of Caldicott Guardians, their role and responsibilities [Online] Available from: https://www.gov.uk/government/publications/national-data-guardian-guidance-on-the-appointment-of-caldicott-guardians-their-role-and-responsibilities [Accessed: 23/06/2025] • Author: ICO, (2025), Your beginner's guide to data protection [Online] Available from: https://ico.org.uk/for-organisations/advice-for-small-organisations/your-beginner-s-guide-to-data-protection/ [Accessed: 23/06/2025] • Author: National Cyber Security Centre, (2025), Small Business Guide: Cyber Security [Online] Available from: https://www.ncsc.gov.uk/collection/small-business-guide [Accessed: 23/06/2025] • Author: NHS Digital, (2025), Data and technology that improves lives [Online] Available from: https://digital.nhs.uk/ [Accessed: 23/06/2025]

	• Author: NHS Digital, (2025), Data Security and Protection Toolkit [Online] Available from: https://www.dsptoolkit.nhs.uk/ [Accessed: 23/06/2025] • Author: NHS Digital, (2022), A Guide to Confidentiality in Health and Social Care [Online] Available from: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/a-guide-to-confidentiality-in-health-and-social-care [Accessed: 23/06/2025] • Author: NICE, (2018), Decision-making and mental capacity [Online] Available from: https://www.nice.org.uk/guidance/ng108 [Accessed: 23/06/2025] • Author: Digital Care Hub, (2025), Advice and support to the adult social care sector on technology, data protection and cyber security [Online] Available from: https://www.digitalcarehub.co.uk/ [Accessed: 23/06/2025]
Suggested Action:	• Encourage sharing the policy through the use of the QCS App
Equality Impact Assessment:	QCS have undertaken an equality analysis during the review of this policy. This statement is a written record that demonstrates that we have shown due regard to the need to eliminate unlawful discrimination, advance equality of opportunity and foster good relations with respect to the characteristics protected by equality law.

Next Steps Mental Healthcare LTD
32 Kingscliffe Street Moston Manchester Lancashire M9 4PG

1. Purpose

1.1 To detail the rights of Service User / Residents relating to confidentiality and data protection and issues that staff need to be aware of when processing confidential information within Next Steps Mental Healthcare LTD.

1.2 This is one of a suite of policies that relates to Data Protection, Information Governance, Data Quality and Security and the Human Rights of Service User / Residents and dovetails to form a framework that ensures full legal compliance and best practice.

1.3

Key Question	Quality Statements
SAFE	QSS4: Involving people to manage risks QSS5: Safe environments
WELL-LED	QSW5: Governance, management and sustainability

1.4 Relevant Legislation

- The Care Act 2014
- Freedom of Information Act 2000
- Human Rights Act 1998
- Data Protection Act 2018
- UK GDPR
- The Health and Social Care (Safety and Quality) Act 2015

2. Scope

2.1 Roles Affected:

- All Staff

2.2 People Affected:

- Service User / Residents

2.3 Stakeholders Affected:

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

3. Objectives

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

3.2 To establish the approach of Next Steps Mental Healthcare LTD to ensuring the confidentiality of personally identifiable information.

3.3 To inform Service User / Residents, their families, legal representatives, stakeholders and Next Steps Mental Healthcare LTD staff about the confidentiality obligations of Next Steps Mental Healthcare LTD and how we intend to meet them.

3.4 To inform staff working for, or on behalf of Next Steps Mental Healthcare LTD of their responsibilities with regards to confidentiality and personally identifiable information and how Next Steps Mental Healthcare LTD will enable these to be met.

4. Policy

4.1 Next Steps Mental Healthcare LTD recognises that we have a duty of confidentiality to the Service User / Residents and staff. We believe that respecting a person's right to a private life, which includes confidentiality, is important in ensuring a trusting, caring and supportive environment where both Service User / Residents and staff are confident that information about them will be protected safely and not shared inappropriately or unnecessarily.

It is the policy of Next Steps Mental Healthcare LTD that we will only share information that is in the best interest of the Service User / Residents and with their consent. Sharing of information will be carried out in line with the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, Mental Capacity Act and Best Interests policies and procedures at Next Steps Mental Healthcare LTD.

We aim to comply with the relevant legislation and include the Caldicott Principles.

4.2 Caldicott Guardian

Next Steps Mental Healthcare LTD understands its obligations to appoint a Caldicott Guardian in line with guidance from the National Data Guardian for Health and Social Care.

Further information is available in the Caldicott Guardian Policy and Procedure.

4.3 Core Principles of Confidentiality

- All staff will ensure that all Service User / Resident information remains confidential. Service User / Residents have the right to expect that personal information held about them is not accessed, used or disclosed improperly
- The same duty of confidentiality applies to personal information about staff with the exception of names and job titles. Information about Directors, which is published, and therefore is a matter of public record, is also excepted
- All staff have the individual responsibility for ensuring that they conform to the Caldicott principles, UK GDPR, Data Protection Act (DPA) 2018 and Article 8 Human Rights Act (HRA) 1998
- Staff must not inappropriately access, misuse or share any information or allow others to do so. Staff are personally liable for deliberate or reckless breaches of the UK GDPR, Data Protection Act and may be liable to disciplinary action and/or prosecution

- Any personal information given or received in confidence for one purpose may not generally be used for a different purpose, or passed to anyone else without the consent of the provider of the information

4.4 The Position of Next Steps Mental Healthcare LTD **on Confidentiality**

- We will share with Service User / Residents, 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 that 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 / Resident or to another individual if this principle is strictly adhered to
- There is a recognition that 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
- Next Steps Mental Healthcare LTD will ensure that personally identifiable information will always be held securely and, when used, treated with respect. This rule will apply regardless of where the information is held
- Although the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act no longer applies to identifiable data that relate to a person once they have died, we respect that any duty of confidence established prior to death continues after the Service User / Resident has died
- All information regarding the Service User / Residents we support will be treated with respect and integrity
- We will be transparent in our approach to ensure that anyone associated with Next Steps Mental Healthcare LTD (whether Service User / Resident, staff or visitor) is fully aware of how, what, when, who and why we share any information about them and source their agreement before doing so

4.5 All relevant staff will be 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. Care Workers will follow the Skills for Care Code of Conduct for Healthcare Support Workers and Adult Social Care Workers in England.

4.6 All staff must sign a confidentiality agreement as part of their contract of employment (a template can be found within the forms section of this policy). The confidentiality agreement also extends to agency and contract workers.

4.7 Responsibilities - Managing Director

- Ensuring that systems and processes are in place for the security of records and they are reviewed to ensure that they remain fit for purpose
- Ensuring that all staff understand this policy at the start of employment and that its importance is reiterated during supervision or team meetings
- Ensuring that staff have received the appropriate training and are competent in their role
- Reviewing, monitoring and auditing practice within Next Steps Mental Healthcare LTD to ensure that staff remain knowledgeable
- Acting on any breaches in confidentiality in a timely manner and notifying the appropriate bodies
- Ensuring that confidentiality rules are never used as a barrier to sharing appropriate information and fulfilling Duty of Candour obligations

4.8 Responsibilities - All staff will ensure the following:

- That information received is **effectively protected** against improper disclosure when it is **received, stored, transmitted and disposed** of
- That confidential information is only accessed if it is appropriate to the job you undertake
- That every effort is made to ensure that Service User / Residents understand how information about them will be used before they supply any confidential information
- That when Service User / Residents give consent to the disclosure of information about them, they understand what will be disclosed, the reasons for disclosure and the likely consequence/s
- That Service User / Residents understand when information about them is likely to be disclosed to others, and that they have the opportunity to withhold their permission
- If disclosing information outside the team that could have personal consequences for the Service User / Resident, that consent is obtained from the Service User / Resident
- If the Service User / Resident 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 / Resident **or someone else from the risk of significant harm)**
  - **They are required by law or by order of a court**
- If required to disclose confidential information, staff will only release as much information as is necessary for the purpose
- That the person(s) to whom information is disclosed understands that it is given to them in confidence which they must respect
- When disclosing confidential information, staff must be prepared to explain and justify the decision. Where there are doubts, they will discuss them with Andy Kershaw
- Queries concerning this policy will be brought to the attention of Andy Kershaw
- During the induction period for new staff, they will be made aware of this policy and their individual responsibilities

5. Procedure

5.1 Next Steps Mental Healthcare LTD will detail with transparency how confidentiality is managed with Service User / Residents, employees and others at the earliest opportunity and seek their agreement, e.g. through existing systems such as recruitment and Next Steps Mental Healthcare LTD assessment processes.

Staff should refer to the Data Privacy templates and the External and Employee Privacy Policy and Procedure for further information that details how information is processed within Next Steps Mental Healthcare LTD.

5.2 Sharing Information With Other Health and Social Care Professionals

Information sharing between partners directly involved in the Service User / Resident's care, and for the purpose of providing that care, is essential to good practice.

Consent from the Service User / Resident for information sharing must be recorded following a discussion with the Service User / Resident or, in the absence of capacity to consent, their designated other.

The principles of sharing information are:

- Only information that needs to be shared
- Only with those who have a clear need to know, and
- There is a lawful basis for sharing information

5.3 General Principles of Confidentiality - Staff will:

- Understand and follow the Caldicott Principles as detailed within the Forms section of this policy
- Be aware that the Data Protection Act 2018 (DPA 2018), and the UK General Data Protection Regulation (UK GDPR) are not barriers 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 and will seek their agreement unless it is unsafe or inappropriate to do so
- Seek advice from Andy Kershaw if they 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. Staff may still share information without consent if, in their judgment, that lack of consent can be overridden in the public interest
- Consider safety and wellbeing. Staff must base 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 shared is necessary for the purpose for which it is being shared, 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
- Staff must keep a record of any decision and the reasons for it (to include what has been shared, with whom and for what purpose), and for a decision not to share

5.4 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 / Resident's consent. This includes family, friends and private carers, and other professionals
- If in doubt, staff will consult the Line Manager or Andy Kershaw, Managing Director
- Conversations relating to confidential matters affecting Service User / Residents will not take place anywhere that they may be overheard by others, i.e. in public places - such as supermarkets, public transport, open plan areas of the office, during training or group supervision where other staff not involved in the Service User / Resident's care are present
- 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 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 Service User /

Resident and their families have in Next Steps Mental Healthcare LTD

- Staff must not pass on any information or make comments to the press or other media. Media enquiries should be referred to the person responsible for handling any media enquiries
- Next Steps Mental Healthcare LTD can refer to the Caldicott Guardian Policy and Procedure for further guidance

5.5 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:

- Staff must verify the identity of the person requesting the information whilst establishing if it can be anonymised (refer to 5.8)
- Information will only be shared on a 'need to know' basis when it is in the best 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 Next Steps Mental Healthcare LTD 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

5.6 Rights of all Service User / Residents

All Service User / Residents 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 / Resident'. The policy of Next Steps Mental Healthcare LTD is to record information in a way that, as far as possible, avoids a need for this exclusion. If the Service User / Resident believes their right to confidentiality is either being breached or undermined, they must have access to the complaint's procedure at Next Steps Mental Healthcare LTD.

Staff should refer to the Subject Access Requests Policy and Procedure for further details.

5.7 Rights of all Staff

All staff may view personal information held by Next Steps Mental Healthcare LTD that relates to them, by applying in writing to their Line Manager or Managing Director, Andy Kershaw.

5.8 Data Security and Quality

- Any record that contains information about an individual must remain confidential unless it is in the public domain. All records must be factual and not include the personal opinions of the person writing the records. Staff should refer to the Record Keeping Policy and Procedure for further details
- Reproduction of information relating to the Service User / Resident (for example photocopying documents) will only be done with the consent of the Service User / Resident
- Confidential information to be posted must be marked 'Private & Confidential, for the attention of the addressee only', and sent by recorded/special delivery

Staff should refer to the guidance contained in the Forms section of this policy for best practice and requirements for data security. However, as a minimum:

- Information held within Next Steps Mental Healthcare LTD will not be shown to unauthorised individuals or be left where unauthorised personnel may access it. All records must be kept in a lockable cabinet in a lockable office, with restricted access
- All written records must be kept securely and only disposed of by shredding, after appropriate timescales. Staff must take care when recording personal identifiable information into personal notebooks or paper during shift handover and ensure the safekeeping and destruction of the information
- Written information also relates to door codes, lockers, key safe numbers and staff rotas. Staff must be provided only with secure information if required to carry out specific tasks in secure areas and locations with restricted access. Secure information must not be recorded on Service User / Resident records for use outside the office or on rotas supplied to staff. Staff must ensure that if they record Service User / Resident information to support the delivery of care, for example a request to cover an unplanned absence, the information is recorded securely and safely destroyed after use
- Any rotas must be returned to the office for confidential disposal
- Any employee who breaches this policy may be subject to disciplinary action

5.9 Social Media

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

5.10 Mental Capacity and Confidentiality

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

5.11 Anonymisation and Pseudonymisation Considerations

Anonymisation

Anonymised information (i.e. where personal information is removed and both the giver and the receiver are unable to identify the Service User / Resident) is not confidential and may be used outside of data protection legislation. However, staff should be aware that information which contains small numbers of person identifiable information may lead to identification. For this reason, all disclosure of anonymised information should be reviewed on a case-by-case basis. Next Steps Mental Healthcare LTD will seek to anonymise collective data about individuals within Next Steps Mental Healthcare LTD.

Pseudonymisation

Pseudonymisation is the practice of removing and replacing actual data with a coded reference (a ‘key’). Next Steps Mental Healthcare LTD will consider this practice where the use of the data needs to relate to individual records, but also needs to retain security and privacy for that individual. There is a higher privacy risk and security risk of the key system as the data will not truly be anonymised.

Personal data that has been pseudonymised can fall within the scope of data protection legislation depending on how difficult it is to assign it to a particular individual.

Further information can be found within the ICO Anonymisation Code of Practice.

5.12 Next Steps Mental Healthcare LTD **Confidentiality**

Suppliers

Staff must extend the principles of confidentiality when considering Next Steps Mental Healthcare LTD sensitive information and the protection of any commercial data.

When Next Steps Mental Healthcare LTD engages a software vendor or data processor it will ensure and evidence that the new supplier adheres to UK GDPR.

Staff and/or external suppliers will ensure that information such as suppliers' prices, performance and costs are not disclosed to other suppliers or unauthorised persons. Next Steps Mental Healthcare LTD could consider requesting that suppliers sign a confidentiality agreement in order to protect the data of Next Steps Mental Healthcare LTD.

If there are any queries about how to support commercially sensitive information, these should be discussed with Andy Kershaw.

Meetings

Next Steps Mental Healthcare LTD has a right to have confidential meetings where information is discussed and then held securely and confidentially. Information held will be in line with the Freedom of Information Act (FOIA) 2000 and UK GDPR, the Data Protection Act 2018.

Complaints and Investigations

Complaints and investigations are treated confidentially and remain so unless there is a legal requirement to release information.

Media

Staff must not pass on any information, or make comments, to the press or other media. Media enquiries should be referred to the person responsible for handling any media enquiries.

5.13 Confidentiality Breach

Unauthorised access, use or disclosure may be in breach of the UK GDPR, DPA 2018, the Human Rights Act, and/or breach the policies of Next Steps Mental Healthcare LTD and may lead to disciplinary action.

Where there has been a breach in confidentiality, this will be recorded on an incident form at Next Steps Mental Healthcare LTD and reported to Andy Kershaw.

Significant breaches will be reported to Andy Kershaw so that reporting to the relevant regulatory, professional bodies and the ICO is considered.

Breaches will be monitored by Andy Kershaw, reflected on with lessons learned and will form part of the quality assurance programme for Next Steps Mental Healthcare LTD.

Staff will refer people to the Complaints, Suggestions and Compliments Policy and Procedure at Next Steps Mental Healthcare LTD.

5.14 The National Cyber Security Centre

Alongside this policy the National Cyber Security Centre has provided a useful resource centre that will assist Next Steps Mental Healthcare LTD in improving and keeping up to date with Cyber Security. The Small Business Guidance is formulated under five steps:

- **Step 1: Backing up your data**
- **Step 2: Protecting your organisation from malware**
- **Step 3: Keeping smartphones and tablets safe**
- **Step 4: Using passwords to protect your data**
- **Step 5: Avoiding phishing attacks**

Alongside this guidance there are additional resources that are available to use. Next Steps Mental Healthcare LTD will make full use of this tool, such as the Cyber Action plan; a link to which is in the Underpinning Knowledge section.

6. Definitions

6.1 Data Protection Act 2018

- The Data Protection Act 2018 is a United Kingdom Act of Parliament that updates data protection laws in the UK
- It sits alongside the UK General Data Protection Regulation and implements the EU's Law Enforcement Directive

6.2 Caldicott

- The Caldicott Principles provide guidance to the NHS and adult social care records on the use and protection of personal, confidential data and emphasises the need for controls over the availability of such information and access to it
- Caldicott Report
- The Caldicott Report made a series of recommendations which led to the requirement for all NHS organisations (and adult social care records from the year 2000) to appoint a Caldicott Guardian who is responsible for compliance with the Caldicott confidentiality principles
- **Caldicott Guardian**
- A senior person responsible for protecting the confidentiality of peoples' health and care information and making sure it is used properly

6.3 Common Law Duty of Confidentiality

- Prohibits the 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. patient

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 that 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, for example, 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

- Information that, if disclosed, could harm or damage the reputation or image of an organisation

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 / Resident 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 / Resident unless the Service User / Resident 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

7. Key Facts - Professionals

Professionals providing this service should be aware of the following:

- Professionals can only tell other people the Service User / Resident's personal information if the Service User / Resident says they can or if they have to
- Professionals can share information without the Service User / Resident's consent if there is a risk of serious harm to the Service User / Resident or other or there is a risk of a serious crime
- When the Service User / Resident dies, the duty of confidentiality will continue to apply, even though the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act no longer 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

8. 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

GOV.UK - Information: To Share or not to Share - The Information Governance Review:

https://www.gov.uk/government/publications/the-information-governance-review

Care Quality Commission - Using surveillance in your care service:

https://www.cqc.org.uk/guidance-providers/all-services/using-surveillance-your-care-service

Durham University - Provides a useful introduction to Anonymisation and Pseudonymisation:

https://www.dur.ac.uk/ig/dp/anonymisation/

Easy Read Online - Your rights about your personal information:

https://www.sldo.ac.uk/media/1821/easy-read-gdpr-info-sheet.pdf

UK Caldicott Guardian Council:

https://www.gov.uk/government/groups/uk-caldicott-guardian-council

Additional Policies:

Suite of Data Protection Policies in the system at Next Steps Mental Healthcare LTD

Outstanding Practice

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

- The wide understanding of the policy is enabled by proactive use of the QCS App
- Robust systems and governance processes ensure that staff and Service User / Resident confidentiality is maintained at all times
- Staff are registered as Dignity Champions and can evidence that they follow the 'Dignity Dos'
- Each person's privacy needs and expectations should be identified, recorded, and met as far as is reasonably possible
- Staff treat Service User / Residents with kindness and respect and maintain Service User / Resident and information confidentiality

Forms

The following forms are included as part of this policy:

Title of form	When would the form be used?	Created by
Staff Confidentiality Agreement - CR07	This agreement is provided to clarify the responsibilities of those employed at this service in respect of maintaining confidential information gathered by the service in the course of its work.	QCS
Caldicott Principles - CR07	To offer guidance to staff around the principles.	QCS

Next Steps Mental Healthcare LTD
32 Kingscliffe Street Moston Manchester Lancashire M9 4PG

Title of form	When would the form be used?	Created by
Data Security Guidance - CR07	To detail the requirements for safe and secure records management.	QCS

Next Steps Mental Healthcare LTD
32 Kingscliffe Street Moston Manchester Lancashire M9 4PG

Staff Confidentiality Agreement - CR07

This agreement is provided to clarify the responsibilities of those employed at Next Steps Mental Healthcare LTD in respect of maintaining confidential information gathered by the service in the course of its work.

Queries and questions relating to this duty should be addressed to either the:

Managing Director

Data Protection Officer

All information given by Service User / Residents to staff is given on the understanding that it will be used solely for providing them with care most suited to their needs. It is the duty of Next Steps Mental Healthcare LTD to ensure that the confidentiality of that information is maintained within the boundaries of the law and professional standards and is not divulged without the consent of the Service User / Resident.

In the course of your work at Next Steps Mental Healthcare LTD, you will have access to person identifiable, confidential data concerning the medical or personal affairs of:

- Service User / Residents and their families/significant others
- Staff of Next Steps Mental Healthcare LTD
- Associated health and social care professionals

Unless acting on practice policy or following the direct instructions of K Bond Healthcare TA Next Steps, or the Managing Director, such information must not be divulged or discussed except in the performance of your normal duties. Breach of confidence, including the improper passing of computer data, may result in disciplinary action, your dismissal, and civil action against you for damages.

In observation of the suite of UK GDPR, Data Protection Policies at Next Steps Mental Healthcare LTD, you must ensure that all records, including computer screens and computer-generated records or paper records of staff or Service User / Resident data are never left where unauthorised persons can view them.

Computer screens must always be cleared when left unattended and you must ensure that you log out of computer systems, removing your password. All passwords to the systems of Next Steps Mental Healthcare LTD must be kept confidential.

No unauthorised use of the Internet or email is allowed.

Information concerning Service User / Residents or team members is strictly confidential and must not be disclosed to unauthorised persons. This obligation continues without end, during and after your employment at Next Steps Mental Healthcare LTD. Disclosures of confidential information or disclosures of any data of a personal nature can result in prosecution for an offence under UK GDPR and the Data Protection Act 2018.

I have read, understand and agree to the terms and conditions set out above:

Signature: Date:

Name:

Next Steps Mental Healthcare LTD
32 Kingscliffe Street Moston Manchester Lancashire M9 4PG

Caldicott Principles - CR07

The Caldicott Principles revised in 2020 are:

Principle 1 - Justify the purpose(s) for using confidential information

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2 - Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 - Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 - Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

In April 2013, Dame Fiona Caldicott reported on her second review of information governance, her report "Information: To Share or Not to Share? The Information Governance Review", informally known as the "Caldicott2 Review", introduced a new 7th Caldicott Principle.

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8 - Inform patients and service users about how their confidential information is used

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

Data Security Guidance - CR07

Physical Location and Security

- Unauthorised staff or members of the public must not be able to gain access to person identifiable information
- Person identifiable information will be held in rooms that conform to health and safety standards in terms of fire safety and safety from flood, theft or environmental damage
- Paper records containing person identifiable information must be stored in locked filing cabinets
- Computers must not be left on view or be accessible by unauthorised staff. Computers must have a secure screen saver function and be switched off when not in use
- Equipment such as fax machines must have a password and be switched off outside office hours if situated in a non-secure area

Fax Machines

Fax machines must only be used to transfer personal information where it is absolutely necessary to do so. The following rules must apply:

- Ensure it is sited in an area that is restricted to those who need to access the information
- The fax is sent to a safe location where only staff who have a legitimate right to view the information can access it
- The sender is certain that the correct person will receive it and that the fax number is correct
- Notify the recipient when you are sending the fax and ask them to acknowledge receipt
- The confirmation of receipt should be checked to ensure the fax has been transmitted to the intended recipient. Where possible, this should be attached to the original document
- Where possible, the NHS number should be used for identification in preference to the Service User / Resident's name and address
- Care is taken in dialling the correct number
- Confidential faxes are not left lying around for unauthorised staff to see
- Only the minimum amount of personal information should be sent
- Use a fax cover sheet that contains a confidentiality statement (example - "This fax is confidential and is intended only for the person to whom it is addressed. If you have received this fax in error, please immediately notify us by telephone on the number above and return the message to us by post. If the reader of this fax is not the intended recipient, you are hereby notified that any distribution or copying of the message is strictly prohibited")
- Frequently used numbers should be programmed into the fax machine 'memory dial' facility. This will minimise the risk of dialling incorrect numbers
- If you receive a call requesting that confidential information be sent via fax, always call the requestor back to confirm the caller's identity using an independent number source
- Always seek advice from your line manager if you are unsure whether or not to send any information via fax
- If it is highly sensitive, ensure that someone is at the receiving end waiting for it

- Ensure that only authorised staff handle confidential information
- If you receive faxes that contain personal information, store them in a secure environment
- Fax machines should be turned off out of hours

Post and Paper Documents

- Incoming mail should be opened away from public areas
- Outgoing mail (both internal and external) should be sealed securely and marked 'Private and Confidential' if it contains person identifiable information. Where possible, send post to a named person
- When sending documents by external post or courier, use a “signed for" delivery service. Use appropriate stationery, such as reinforced envelopes or document wallets when necessary. Check that the address is typed or written clearly in indelible ink
- Send documents only to known, named, authorised personnel marked “Confidential" and use a "signed for" or "recorded delivery" service
- Confidential information must not be left unattended at any time
- Information should be shredded when it is no longer required (e.g. post-it notes, messages)
- Staff should ensure that they comply with the guidance on the retention of confidential information

PCs, Laptops and Memory Sticks

- Do not share log-ins and passwords with anyone
- Computer screens must not be left on view so that members of the general public or staff who do not have a justified need to view the information can see personal data
- PCs or laptops should be locked using the "control, alt, delete" function or switched off when you are away from your desk for any length of time
- Information should be held on the network servers of Next Steps Mental Healthcare LTD, not stored on local hard drives or removable media
- Any information must not be saved or copied into any PC or media that is “outside Next Steps Mental Healthcare LTD”
- The number of staff with access privileges should be kept to a minimum (e.g. administrator access to the system)

Emails

- The email system of Next Steps Mental Healthcare LTD should not be used to transfer commercially sensitive or personal identifiable information outside of Next Steps Mental Healthcare LTD unless this information is encrypted
- All person identifiable information sent by email must be sent securely
- Email disclaimers should be used appropriately. Remember, adding a disclaimer routinely to all emails may make them meaningless through overuse (example - "Privileged and/or confidential information may be contained in this message. If you are not the original addressee indicated in this message (or responsible for delivery of the message to such person) you may not copy or deliver this message to anyone. In such cases please delete this message and notify us immediately. Opinions, conclusions and other information expressed in this message are not given or endorsed by my employer unless otherwise indicated by an authorised representative independently of this message")

Telephone Calls

- Do not make confidential telephone calls where you can be overheard (e.g. Reception)

- When you receive a call check to ensure that you are speaking to the correct person, ring back (where possible) to confirm someone's identity

Remote Working

- There may be times when staff need to work from another location or whilst travelling. This may mean that staff carry confidential information either on a laptop or in paper form
- Taking home or removing paper records that contain person identifiable or confidential information from the premises is discouraged
- Where there is no choice, staff must minimise the amount of person identifiable information that is taken away and ensure the following: information is carried in a sealed non-transparent container, e.g. a windowless envelope, bag, etc. and it is kept out of sight whilst being transported
- To ensure safety, staff must keep such records on their person at all times when travelling and ensure that they are kept in a secure place if they take them to another location
- Confidential information must be safeguarded at all times and kept in lockable locations
- When away from the premises, all policies and procedures remain relevant
- Staff must not use or store person identifiable or confidential information on a privately owned computer or device

To Summarise, Confidentiality Dos and Don'ts

Dos

- Do safeguard the confidentiality of all person identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of Next Steps Mental Healthcare LTD
- Do clear your desk at the end of each day, keeping all non-digital records containing person identifiable or 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 person identifiable or business 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 person identifiable or confidential information and ensure that they have a need to know
- Do share only the minimum information necessary
- Do transfer person identifiable or confidential information securely
- Do seek advice if you need to share Service User / Resident/person identifiable information without the consent of the Service User / Resident's/identifiable person's consent, and record the decision and any action taken
- Do report any actual or suspected breaches of confidentiality
- Do participate in induction, training and awareness raising sessions on confidentiality issues

Don'ts

- Don't share passwords or leave them lying around for others to see
- 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 person identifiable 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