CR07 - Data Protection and Confidentiality Policy and Procedure

Abbeyfield Tamar Extra Care Society
11 Brest Road, Plymouth, PL6 5XN

Data Protection - Policies

Last reviewed: 25 August 2026
Version: 26.11.26-01.43.59

Review Sheet

Last Reviewed	Last Amended	This policy will be reviewed as needs require or at the following interval:
25 Aug 2026	25 Aug 2026	Annual

Business Impact: Minimal action required. Circulate information amongst LOW relevant parties.

Reason for this Review: Scheduled review

Changes Made: Yes

This policy details the rights of Service User / Residentss and staff in relation to confidentiality and data protection and the responsibilities of staff when handling personal and confidential information.

The policy has been reviewed following the implementation of the Data (Use and Access) Act 2025. Wording relating to consent and information sharing has been clarified to ensure that staff understand that consent is not always required where there is another lawful and justifiable basis for sharing information.

Summary: References to NHS Digital have been updated to NHS England where appropriate. Terminology relating to special category data has also been updated.

The policy has been strengthened to reflect current information governance risks associated with electronic care records, mobile devices, remote working, email, photographs, videos, screenshots, personal devices, cyber security, phishing and artificial intelligence.

References and further reading links have also been reviewed and

The Care Act 2014 Freedom of Information Act 2000 Human Rights Act 1998 Relevant Legislation:
Data Protection Act 2018 UK GDPR The Health and Social Care (Safety and Quality) Act 2015 Health and Social Care (Safety and Quality) Act 2015 Data (Use and Access) Act 2025

Author: NHS England, formerly NHS Digital, (2025), Code of

Practice on Confidential Information [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/code-of- practice-on-confidential-information [Accessed: 25/08/2026] 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: 25/08/2026] 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: 25/08/2026] Author: ICO, (2025), Getting Started with Data Protection - A step- by-step guide [Online] Available from: https://ico.org.uk/for- Underpinning Knowledge: organisations/advice-for-small-organisations/your-beginner-s-guide- to-data-protection/ [Accessed: 25/08/2026] Author: National Cyber Security Centre, (2025), Small Business

Guide: Cyber Security [Online] Available from:

https://www.ncsc.gov.uk/collection/small-business-guide [Accessed:
25/08/2026] Author: NHS England, formerly NHS Digital, (2025), Data and

Technology that Improves Lives [Online] Available from:
https://digital.nhs.uk/ [Accessed: 25/08/2026] Author: NHS England, formerly NHS Digital, (2025), Data Security

and Protection Toolkit [Online] Available from:
https://www.dsptoolkit.nhs.uk/ [Accessed: 25/08/2026] Author: NHS England, formerly 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- Author: NICE, (2018), Decision-Making and Mental Capacity [Online] Available from: https://www.nice.org.uk/guidance/ng108 [Accessed: 25/08/2026] 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: 25/08/2026]

Suggested Action: Encourage sharing the policy through the use of the QCS App

QCS have undertaken an equality analysis during the review of this policy. This statement is a written record that demonstrates that we Equality Impact Assessment: 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.

1. Purpose

1.1 About Abbeyfield Tamar Extra Care Society

Tamar House is a purpose built home providing exceptional levels of residential care on the Northern edge of Plymouth. Built in 1987, this two-storey building is conveniently located in Derriford, close to the hospital, transport routes and other amenities.

Tamar House provides a caring home for 29 residents who all enjoy their own private rooms, most with private toilet and washbasin facilities. The home also benefits from two fully en-suite bedrooms, beautifully designed sensory bathrooms on both floors and dedicated shower rooms, offering residents comfort, privacy and a relaxing bathing experience. There are a number of comfortable communal areas for residents and a welcoming dining room on the ground floor. Tamar House is fully accessible to service users with physical disabilities with a lift, and a stair lift, between floors. What are the values of Abbeyfield Tamar Extra Care Society?

The Home aims to:

- Offer skilled care to enable people who live here to achieve their optimum state of health and well-being.
- Treat all people who live and work at The Home and all people who visit with respect at all times.
- Uphold the human and citizenship rights of all who live, work and visit here.
- Support individual choice and personal decision-making as the right of all Service Users.
- Respect and encourage the right of independence of all Service Users.
- Recognise the individual uniqueness of Service Users, staff and visitors, and treat them with dignity and respect at all times.
- Respect individual requirement for privacy at all times and treat all information relating to individuals in a confidential manner.
- Recognise the individual need for personal fulfilment and offer individualised programmes of meaningful activity to satisfy the need of all residents and staff.
- Tamar House aims to provide high-quality, person centred residential care that promotes the dignity, independence, wellbeing, and rights of all residents. We are committed to delivering care that is safe, effective, caring, responsive, and well led, in accordance with the requirements of the Health and Social Care Act 2008 and associated regulations.

objectives:

- To provide safe care - we aim to protect residents from harm, abuse, and neglect by maintaining robust safeguarding procedures, effective risk assessments, and safe systems of care, including medication management and infection prevention and control.
- To deliver effective and individualised care - We will assess each resident's needs comprehensively and develop personalised care plans that reflect their preferences, choices, and goals. We will ensure that all staff are appropriately trained, competent, and supported to deliver high standards of care.
- To promote dignity, respect and compassion - We are committed to treating all residents with kindness, respect, and dignity at all times, ensuring their privicy is upheld and their emotional and social wellbeing is supported.
- To provide responsive and person centred services - We will tailor our services to meet the diverse and changing needs of residents, responding promptly to feedback, concerns, and compliments, and encouraging meaningful activities and engagement.
- To ensure effective leadership and governance - We will maintain strong leadership and clear accountability, regularly monitoring and improving the quality of our services through audits, feedback, and continuous development.

- To promote independence and choice - We will support residents to maintain their own independence wherever possible, enabling them to make informed decisions about their care and daily lives.
- To uphold legal rights and compliance - We will operate in accordance with relevant legislation, including the Mental Capacity Act 2025, ensuring that consent is obtained and residents rights are protected at all times.
- To engage with families and the wider community - We will communicate openly with families, carers, and representatives, encouraging their involvement in care planning and fostering strong community links to enhance residents' quality of life. Tamar House is committed to continuous improvement and to meeting and exceeding the standards set by the Care Quality Commission. We strive to create a safe, welcoming, and supportive environment where residents can live fulfilling lives.

1.2 To detail the rights of Service User / Residentss, staff and other individuals in relation

to confidentiality and data protection and the responsibilities of staff when accessing, recording, using, storing, sharing or disposing of personal and confidential information within Abbeyfield Tamar Extra Care Society.

1.3 This is one of a suite of policies relating to data protection, information governance,

data quality, information security and the human rights of Service User / Residents and others whose information is processed by Abbeyfield Tamar Extra Care Society. These policies work together to support legal compliance and good practice.

1.4 To support Abbeyfield Tamar Extra Care Society in meeting the following Quality

Statements:

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

1.5 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 Health and Social Care (Safety and Quality) Act 2015 Data (Use and Access) Act 2025

2. Scope

2.1 Roles Affected:

All Staff Anyone working for or on behalf of Abbeyfield Tamar Extra Care Society Contractors Agency Staff All Care and Support staff

2.2 People Affected:

Service User / Residents

2.3 Stakeholders Affected:

Family Advocates Commissioners External health professionals Local Authority NHS Local procurement, purchasing and supplies services

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 Abbeyfield Tamar Extra Care Society to protecting

personal and confidential information.

3.3 To inform Service User / Residents, their families, legal representatives, stakeholders

and staff about the confidentiality and data protection obligations of Abbeyfield Tamar Extra Care Society staff and how these obligations will be met.

3.4 To inform staff working for, or on behalf of Abbeyfield Tamar Extra Care Society of their

responsibilities in relation to confidentiality, data protection and information security and how Abbeyfield Tamar Extra Care Society will support these responsibilities to be met.

3.5 To support lawful, necessary and proportionate information sharing and to ensure that

confidentiality is not used as a barrier to safe care and support, safeguarding or compliance with a legal duty.

4. Policy

4.1 Abbeyfield Tamar Extra Care Society recognises that it has a duty of confidentiality to

Service User / Residentss and staff. Respecting a person’s right to a private life, which includes confidentiality and is important in ensuring a trusting, caring and supportive environment. Service User / Residents and staff must be confident that information about them will be protected and will not be accessed, used or shared inappropriately or unnecessarily.

It is the policy of Abbeyfield Tamar Extra Care Society that personal and confidential information will only be accessed, used or shared for a clear and legitimate purpose and where there is an appropriate lawful and justifiable basis.

Consent will be sought where consent is the appropriate basis for the proposed use or disclosure. However, consent is not always required. Information may be used or shared without consent where this is necessary and justified for individual care, safeguarding, compliance with a legal obligation or court order, protection from serious harm, prevention or detection of serious crime or another overriding public interest.

Information sharing will be carried out in accordance with the UK General Data Protection Regulation, the Data Protection Act 2018, as amended, the Data (Use and Access) Act 2025, the common law duty of confidentiality, the Mental Capacity Act 2005 and other applicable legal, safeguarding and professional duties. Staff must also follow the relevant Mental Capacity and Best Interests policies and procedures at Abbeyfield Tamar Extra Care Society.

regard to the Caldicott Principles when using or sharing confidential health and care information.

4.2 Caldicott Guardian

Guardian where required by guidance issued by the National Data Guardian for Health and Social Care.

The Caldicott Guardian will support appropriate decision-making about the use and sharing of confidential health and care information. This includes supporting staff to protect confidentiality while ensuring that confidentiality is not used as an inappropriate barrier to sharing information for individual care or another lawful and justified purpose.

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

4.3 Core Principles of Confidentiality

All staff will protect the confidentiality of information relating to Service User / Residents and will only access, use or share that information where they are authorised to do so and where it is necessary for a legitimate purpose 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 The same principles apply to personal and confidential information about staff. Staff names, job titles and professional roles may be used or disclosed where necessary for legitimate operational, regulatory or public-facing purposes. Other staff information must not be accessed, used or shared without appropriate authority All staff have an individual responsibility to comply with this policy and applicable data protection, confidentiality, information security and professional requirements. Staff handling confidential health and care information must also have regard to the Caldicott Principles Personal information obtained for one purpose must not generally be used for an incompatible purpose. Confidential information must not be shared unless the person has consented, the sharing is within their reasonable expectations for individual care, or there is another lawful and justifiable basis for disclosure

Staff must not inappropriately access, misuse, alter, destroy or share information or enable another person to do so. A deliberate, reckless or negligent breach may result in disciplinary action. Certain conduct may also constitute a criminal offence or result in referral to a professional regulator or another relevant authority

4.4 The Position of Abbeyfield Tamar Extra Care Society on Confidentiality

We will provide Service User / Residentss with the information they are entitled to receive about their health, care, support and treatment in a sensitive and accessible way. Information may be shared with families, carers, advocates or representatives where the person has agreed, where the recipient has lawful authority, or where there is another lawful and justifiable basis for sharing Confidential information will not be used for an incompatible purpose or shared with another person unless there is an appropriate lawful and justifiable basis. Consent is one basis for sharing but is not always required Information may be shared without consent where this is required or permitted by law, ordered by a court, necessary to safeguard a child or adult at risk, necessary to prevent or respond to serious harm or serious crime, justified in the public interest or otherwise permitted under the procedures set out in this policy Breaches of confidentiality may be deliberate or unintentional. They may result from conversations being overheard, records being left unattended, information being sent to the wrong recipient, inappropriate access to electronic records, loss of a device, weak information security or information being entered into an unauthorised digital or artificial intelligence system. The consequences may be serious for the individuals concerned and for Abbeyfield Tamar Extra Care Society technical measures to protect personal and confidential information. The required safeguards apply regardless of whether information is held on paper, within an electronic care record, on an approved mobile device or in another authorised system or location Although the UK GDPR and Data Protection Act 2018 do not apply to information relating to a deceased person, any duty of confidence established before death may continue after the person has died. Other legal restrictions may also apply, including those governing access to the health records of deceased people All information regarding the Service User / Residentss we support will be treated with respect and integrity We will be transparent about how and why personal information is used and shared. People will be provided with relevant privacy information and, where appropriate, will be informed about a particular disclosure. Information may be withheld about a disclosure where informing the person would be unlawful, unsafe or likely to prejudice the purpose of the disclosure

4.5 Relevant staff must comply with the standards and codes issued by their professional

regulator or professional body, including, where applicable, the General Medical Council, Nursing and Midwifery Council, General Pharmaceutical Council, Health and Care Professions Council and Social Work England

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. This requirement also applies to agency and contract workers where appropriate.

Signing a confidentiality agreement does not replace the requirement for induction, information governance training, appropriate access controls or ongoing compliance with this policy.

4.7 Responsibilities - Registered Manager

Ensuring that appropriate systems and processes are in place to protect paper and electronic records and that these are reviewed to ensure they remain secure and 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 Abbeyfield Tamar Extra Care Society to ensure that staff remain knowledgeable Ensuring that actual or suspected confidentiality, data protection or information security incidents are contained, recorded, assessed and escalated without delay. This includes notifying the Data Protection Officer, Caldicott Guardian, senior management or other relevant bodies where required, ensuring that confidentiality is not used as an inappropriate barrier to sharing information for individual care, safeguarding, compliance with a legal duty, Duty of Candour or another lawful and justified purpose ensuring that access to personal and confidential information is limited to appropriately authorised people and that access rights are reviewed when roles or employment circumstances change ensuring that staff know how and when to obtain advice from the Registered Manager, the Data Protection Officer, Caldicott Guardian or another appropriately authorised person.

4.8 Responsibilities - All staff will ensure the following:

Information must be protected against unauthorised or inappropriate access, alteration, loss, use or disclosure when it is created, received, accessed, recorded, stored, shared, transmitted, retained and disposed of. Staff must only access information that they are authorised to access and need for the proper performance of their role. Curiosity, personal interest or the ability to access a record does not provide authority to view it, reasonable steps must be taken to ensure that Service User / Residents understand how information about them will be used and shared, including by directing them to the relevant privacy information. Where consent is relied upon, staff must ensure that it is informed, specific and freely given by a person with capacity or lawful authority to make the relevant decision. The person must understand what information will be shared, with whom, for what purpose and the reasonably foreseeable consequences. Where appropriate, Service User / Residents must be informed about proposed information sharing and given an opportunity to express their views or object. An objection must be considered and recorded but will not necessarily prevent sharing where there is another lawful and justifiable basis. Before sharing confidential information outside the direct care team, staff must establish that the proposed recipient is authorised to receive it and that there is an appropriate lawful and justifiable basis for disclosure. Where staff are unsure, they must seek advice before sharing unless urgent disclosure is necessary to prevent serious harm.

If the Service User / Residents withholds consent, or if consent cannot be obtained

for whatever reason, disclosures may be made only where:
The disclosure is required or permitted by legislation The disclosure is required by a court order The information is necessary for individual care and the sharing is within the person's reasonable expectations The disclosure is necessary to safeguard a child or adult at risk The disclosure is necessary to protect the person or another individual from serious harm The disclosure is necessary for the prevention, detection or investigation of serious crime The disclosure is otherwise justified in the public interest Staff must seek appropriate advice where the justification is unclear and must record the decision and rationale. Staff will only share information that is necessary, relevant and proportionate for the identified purpose Where appropriate, staff will ensure that the recipient understands that the information is confidential and must be protected from unauthorised use or further disclosure Staff must be able to explain and justify a decision to share or not to share information. The record must include the reason for the decision, what was shared, with whom, for what purpose and any advice obtained. Where there is doubt, staff must discuss the matter with Registered Manager Questions or concerns about this policy or a proposed disclosure must be raised with Registered Manager. Where necessary, advice should also be obtained from the Data Protection Officer, Caldicott Guardian, safeguarding lead or another appropriately authorised person During induction, new staff will be made aware of this policy, their individual responsibilities and how to report a concern, incident or suspected breach

5. Procedure

5.1 Abbeyfield Tamar Extra Care Society will explain, at the earliest appropriate

opportunity, how personal and confidential information relating to Service User / Residents, employees and others will be collected, used, stored and shared. This information will be provided through appropriate privacy information and existing processes, including recruitment and Abbeyfield Tamar Extra Care Society assessment processes.

Consent or agreement will be sought where this is the appropriate basis for the processing. Where information is processed on another lawful basis, the person will still be informed unless a lawful exception applies.

Staff should refer to the Data Privacy templates and the External and Employee Privacy Policy and Procedure for further information about how personal information is processed within Abbeyfield Tamar Extra Care Society.

5.2 Sharing Information With Other Health and Social Care Professionals

Information sharing between health and social care professionals directly involved in the Service User / Residents's care, for the purpose of providing that care, is essential to safe and effective practice.

Where consent is the appropriate basis for sharing information, the discussion and the person's decision must be recorded.

For individual care, relevant confidential information may be shared with professionals who have a legitimate relationship with the person where the sharing is necessary, proportionate and within the person's reasonable expectations. In these circumstances, implied consent may provide a basis for sharing confidential information, but an appropriate lawful basis under data protection law must still apply.

Where a person lacks capacity to make the relevant decision, staff must follow the Mental Capacity and Best Interests policies and procedures. Another person may only make the decision where they have relevant lawful authority, such as a valid and applicable health and welfare lasting power of attorney or court-appointed deputyship. A family member, carer or "designated other" does not automatically have authority to consent on the person's behalf.

The principles of sharing information are:

Only share information that is necessary, relevant and proportionate for the identified purpose Only share information with an identified and appropriately authorised person who has a clear need to know Ensure that there is an appropriate lawful basis under data protection law and, where confidential information is involved, an appropriate basis for meeting or setting aside the common law duty of confidentiality Verify the identity and authority of the intended recipient Ensure that the information is accurate and up to date where necessary for the purpose Use an approved and secure method of communication Record what was shared, with whom, for what purpose and the justification for sharing

5.3 General Principles of Confidentiality - Staff will:

Understand and follow the Caldicott Principles, where applicable, as detailed within the Forms section of this policy Be aware that the Data Protection Act 2018 and UK GDPR, as amended by the Data (Use and Access) Act 2025, are not barriers to appropriate information sharing. They provide a framework for ensuring that personal information about living individuals is used and shared lawfully, fairly, transparently and securely Understand that identifying a lawful basis under data protection law does not, by itself, remove the common law duty of confidentiality. Where confidential information is involved, staff must also ensure that there is consent, implied consent within the person's reasonable expectations for individual care, a legal requirement or another justifiable basis for disclosure Be open and honest with the person from the outset about why, how and with whom their information is likely to be shared. Families, carers or representatives should be included where the person agrees, where they have lawful authority or where there

is another appropriate basis. Information about a proposed disclosure may be withheld where informing the person would be unlawful, unsafe or likely to prejudice the purpose of the disclosure Seek advice from Registered Manager where there is doubt. Where appropriate, advice should also be obtained from the Data Protection Officer, Caldicott Guardian or safeguarding lead. The person's identity should not be disclosed when seeking advice unless it is necessary to understand and resolve the matter Share information with consent where consent is appropriate. Where a person objects to information sharing, staff must consider and record their wishes. Information may still be shared where there is another lawful and justifiable basis, including individual care within the person's reasonable expectations, safeguarding, legal obligation, court order, prevention of serious harm or serious crime, or an overriding public interest Consider safety and wellbeing. Information-sharing decisions must take account of the safety and wellbeing of the person and others who may be affected by the decision Ensure that information sharing is necessary, proportionate, relevant, accurate, timely and secure. Information must only be shared with people who need it for the identified purpose and must be accurate and up to date where necessary Keep a record of the decision to share or not to share information and the reasons for the decision. Where information is shared, the record must include what was shared, with whom, for what purpose and the method used

5.4 Maintaining Confidentiality

All information regarding the people Abbeyfield Tamar Extra Care Society support will be treated with respect and integrity Personal and confidential information must not be disclosed verbally, in writing, electronically or by any other means unless there is an appropriate lawful and justifiable basis. Family members, friends and carers do not have an automatic right to receive information. Information may be shared with health and social care professionals involved in individual care where this is necessary, proportionate and within the person's reasonable expectations Where there is doubt, staff must consult their Line Manager or Registered Manager. Advice should be escalated to the Data Protection Officer, Caldicott Guardian or safeguarding lead where appropriate Conversations and meetings concerning confidential matters must take place in a setting that protects privacy. Staff must consider the risk of being overheard in public places, shared offices, vehicles, training, group supervision, telephone calls, video calls and when working remotely. Information must not be discussed in the presence of people who are not involved in the person's care or otherwise authorised to receive it Paper records, correspondence, timesheets, rotas and other documents containing personal or confidential information must be kept secure when not in use. Such information must not be left visible or unattended in vehicles, public places or other insecure locations Staff must not disclose confidential information without appropriate authority or justification. Where disclosure without consent is necessary, staff must share only the minimum information required, use a secure method and record the decision and rationale Staff must not disclose information or make comments to the press, social media or other media on behalf of Abbeyfield Tamar Extra Care Society unless authorised to

do so. Media enquiries must be referred to the person responsible for handling them and Procedure for further guidance where applicable

5.5 Safeguarding, The Care Act and Confidentiality

Where an adult safeguarding concern arises, relevant information may need to be shared to prevent abuse or neglect, assess risk, support a safeguarding enquiry or contribute to a Safeguarding Adult Review.

Decisions about what information should be shared and with whom must be made on a case-by-case basis, in accordance with the Care Act 2014, other applicable legislation, local safeguarding procedures and this policy. Staff must not assume that consent is always required before sharing information for safeguarding purposes. Staff must verify the identity and authority of the person requesting information and consider whether the safeguarding purpose can be met by sharing anonymised or pseudonymised information. Refer to section 5.11 Information will only be shared with people who need it for the safeguarding purpose. The information shared must be necessary, relevant and proportionate. Where the adult lacks capacity to make the relevant decision, staff must follow the Mental Capacity and Best Interests policies and procedures Confidentiality must not be confused with secrecy The adult's views and wishes should be sought and respected wherever it is appropriate and safe to do so. However, information may be shared without consent where there is

another lawful and justifiable basis. This may include where:

Other people are or may be at risk of abuse or neglect The adult is at risk of serious harm The adult lacks capacity to make the relevant decision The adult may be subject to coercion, control or undue influence A serious crime has been committed or may be prevented The alleged abuse or neglect involves a member of staff, volunteer or person in a position of trust There is a statutory duty, court order or other legal requirement to disclose The disclosure is otherwise justified in the public interest Staff must not give assurances of absolute confidentiality where there are concerns about abuse or neglect. People should be told, where appropriate and safe, that information may need to be shared to protect them or another person Staff must record the safeguarding information-sharing decision, including the person's views, the information shared or withheld, the recipient, the purpose, the justification and any advice obtained Urgent and necessary information sharing must not be delayed solely because consent cannot be obtained or because advice is not immediately available. Staff must share proportionately, follow emergency and safeguarding procedures and record the action taken

5.6 Rights of all Service User / Residents

All Service User / Residentss have the right to request access to personal information held about them by Abbeyfield Tamar Extra Care Society. A request may be made verbally or in

writing and must be recognised and handled as a subject access request even if the person does not use that term.

Access may only be restricted or refused where an exemption or other lawful restriction applies. This may include circumstances where disclosure of health or social care information would be likely to cause serious harm to the physical or mental health of the person or another individual, or where disclosure would reveal personal information about another person who has not consented and it would not be reasonable to disclose it without their consent.

Information must not be withheld simply because it may be upsetting, critical or uncomfortable to read. Any decision to withhold information must be considered on a case- by-case basis, recorded and referred to the Data Protection Officer or another appropriately authorised person. If the Service User / Residents believes that their confidentiality or data protection rights have been breached or undermined, they must be given access to the data protection complaints procedure at Abbeyfield Tamar Extra Care Society.

Staff should refer to the Subject Access Requests Policy and Procedure for further details. Staff must forward any request for access without delay to the person responsible for managing subject access requests.

Data protection complaints must be handled in accordance with the relevant Complaints Policy and Procedure. Abbeyfield Tamar Extra Care Society must provide an accessible way for people to make a data protection complaint, acknowledge receipt within 30 days and, without undue delay, investigate the complaint, keep the person appropriately informed and communicate the outcome.

5.7 Rights of all Staff

All staff have the right to request access to personal information held about them by should be forwarded without delay to the person responsible for managing subject access requests.

Staff should refer to the Subject Access Requests Policy and Procedure for further details. A request for access must be handled confidentially and must not result in unfair treatment of the member of staff making the request.

5.8 Data Security and Quality

Records containing personal or confidential information must be protected from unauthorised access, use, alteration, loss or disclosure. Information that is publicly available must still be handled appropriately where it constitutes personal data or is combined with other information Records must be accurate, relevant, legible, complete and recorded as soon as reasonably practicable. Facts, professional opinions, information provided by another person and decisions must be clearly distinguished. Staff should refer to the Record Keeping Policy and Procedure for further details Personal or confidential information must only be copied, printed, downloaded, exported, photographed or otherwise reproduced where this is authorised and necessary for a legitimate purpose. Only the minimum information required must be reproduced, and all copies must be protected and disposed of securely when no longer required

Before confidential information is posted, staff must verify the recipient's name and address. The envelope must be securely sealed and marked "Private and Confidential – for the Attention of the Addressee Only" where appropriate. A postal method proportionate to the sensitivity and risk of the information must be used, including tracked, recorded or special delivery where required Staff should refer to the guidance contained in the Forms section of this policy and the relevant information security, record keeping, mobile working and cyber security policies.

As a minimum:

Information must not be shown or made available to unauthorised individuals or left where an unauthorised person may access it. Paper records must be stored in a secure, access-controlled location, using locked cabinets or rooms where appropriate. Electronic records must only be held within approved systems with appropriate access controls Paper records must be kept securely and retained in accordance with the applicable retention schedule. When authorised for destruction, they must be disposed of using an approved confidential waste or cross-cut shredding process Personal or confidential information must not be recorded in personal notebooks or on loose paper unless this is necessary, authorised and no approved alternative is available. Any temporary record must be protected, transferred to the official record where required and securely destroyed as soon as it is no longer needed Door codes, alarm codes, locker codes, key-safe numbers, passwords and other security credentials must only be provided to authorised people who require them for their role. They must not be recorded in care records, rotas, handover documents or other locations where an unauthorised person may obtain access Where personal information must be provided to arrange or deliver care, including when covering an unplanned absence, only the minimum necessary information must be shared through an approved secure method. Any temporary copy must be securely destroyed or deleted when it is no longer required Paper rotas containing personal or confidential information must be returned for confidential disposal or destroyed using another approved method. Electronic copies must be securely deleted when no longer required, in accordance with the applicable retention arrangements Any employee who breaches this policy may be subject to disciplinary action. Actual or suspected incidents must also be reported immediately in accordance with the data breach and incident-reporting procedures Electronic care Records Electronic care records must only be accessed through systems approved by Staff must use their own authorised account. Usernames, passwords, access tokens and multifactor authentication credentials must not be shared Access must be limited according to role and need. The ability to locate or open a record does not provide authority to view it Staff must lock the screen or sign out when leaving a device unattended Entries must be accurate, attributable to the person making the entry and recorded at the time of the event or as soon as reasonably practicable Records must not be deleted, overwritten or altered in a way that conceals the original entry. Corrections must be made using the approved amendment, addendum or "mark in error" function so that an appropriate audit trail is preserved Suspected unauthorised access, incorrect records, unavailable information, delayed synchronisation or loss of access to clinically important information must be reported without delay

Mobile Phones and Tablets

Personal or confidential information must only be accessed or recorded on mobile phones or tablets approved by Abbeyfield Tamar Extra Care Society Approved devices must use appropriate access controls, encryption, supported software, security updates and remote-locking or wiping arrangements where available Devices must not be left unattended or visible in an insecure location Loss, theft, suspected compromise or unauthorised access must be reported immediately Personal devices must not be used to photograph, record, store, access or transmit personal or confidential information unless their use has been formally authorised and is governed by an approved bring-your-own-device arrangement. Remote Working Staff working remotely must use approved systems, devices and secure access methods Screens, documents and conversations must be protected from being seen or overheard by family members, visitors or members of the public Personal or confidential information must not be stored locally, printed or removed from an approved system unless this is authorised and necessary Paper or electronic information must not be left unattended in a vehicle, hotel, shared workspace or other insecure location Email and Electronic Communication Only approved organisational email, messaging and file-transfer systems may be used to send personal or confidential information Staff must verify the recipient, address and attachment before sending information Information must be encrypted or otherwise protected where required by the sensitivity of the information and the approved communication arrangements Personal email accounts, consumer messaging applications and unauthorised cloud-storage services must not be used for organisational personal or confidential information Misdirected emails or messages must be reported immediately and appropriate steps taken to contain the incident Screenshots and Screen Recordings Staff must not take screenshots, photographs or screen recordings of electronic care records or other personal or confidential information unless this is specifically authorised and necessary for an identified purpose An authorised screenshot or recording must contain the minimum information necessary, be transferred and stored securely and be deleted when it is no longer required Screenshots must not be used as a substitute for making an appropriate entry in the official care record Cybersecurity and Phishing Staff must follow organisational requirements concerning passwords, multifactor authentication, software updates, malware protection and secure use of networks and devices Unexpected links, attachments, requests for credentials, payment requests or unusual information requests must be treated with caution Suspected phishing, malware, account compromise or other cyber security incidents must be reported immediately. Staff must not continue interacting with a suspicious

message or system unless instructed by an authorised person Artificial Intelligence (AI) Staff must not enter, upload, dictate, copy or otherwise disclose personal or confidential information to a public or unauthorised artificial intelligence system Artificial intelligence tools must only be used where they have been formally approved by Abbeyfield Tamar Extra Care Society for the intended purpose Before an artificial intelligence system that processes personal information is introduced, Abbeyfield Tamar Extra Care Society must consider the need for a Data Protection Impact Assessment and any applicable clinical safety, information security, equality, procurement and governance assessments Information or content produced by artificial intelligence must not be assumed to be accurate. Where approved AI output is used for care or decision-making, it must be reviewed by an appropriately competent person and any limitations, corrections and relevant decisions must be recorded Artificial intelligence must not be used to make a solely automated decision that has a legal or similarly significant effect on a person unless the use is lawful, authorised and subject to the required safeguards

5.9 Social Media

Staff must not disclose personal or confidential information relating to Service User / Residents, staff or others through social media, online forums, blogs, messaging groups or other public or private online channels unless this has been specifically authorised for a legitimate organisational purpose.

This restriction applies even where names have been removed if the person could still be identified from the circumstances, images, location, dates or other information.

Staff must not use personal social media accounts or personal devices to publish photographs, videos, audio recordings, screenshots or information obtained through their work.

Photographs, Videos and Audio Recordings

Photographs, videos or audio recordings of Service User / Residents must only be created for a clear and authorised purpose. The appropriate consent or other lawful and justifiable basis must be established and recorded before the recording is made or used.

Only approved equipment and systems may be used. The recording must be stored securely, accessed only by authorised people, retained only for as long as necessary and securely deleted in accordance with the applicable retention arrangements.

A person’s agreement to a photograph or recording does not automatically include agreement to publication on social media, a website, promotional material or another platform. The intended uses must be explained and authorised separately where required.

Nothing in this section prevents a member of staff from making a lawful protected disclosure, raising a safeguarding concern, reporting wrongdoing, cooperating with a regulator or exercising another legal right. Staff must use the appropriate authorised reporting route and must not disclose more personal information than is necessary.

5.10 Mental Capacity and Confidentiality

The Mental Capacity Act 2005 applies where there is reason to doubt whether an adult has capacity to make a particular decision at the time the decision needs to be made. Capacity must be presumed unless it is established otherwise, and all practicable steps must be taken to support the person to make the decision for themselves.

Where a person lacks capacity to make a decision about the use or sharing of their information, staff must act in accordance with the Mental Capacity Act 2005, its Code of Practice and the Mental Capacity and Best Interests policies and procedures at Abbeyfield Tamar Extra Care Society.

A family member, carer or nominated contact does not automatically have legal authority to consent to the use or sharing of information on behalf of an adult who lacks capacity. Staff must establish whether another person holds relevant authority, such as a valid and applicable health and welfare lasting power of attorney or court-appointed deputyship.

Where no authorised representative has relevant decision-making authority, the decision must be made in the person's best interests where the Mental Capacity Act applies. The person must be involved as far as possible, and relevant family members, carers, advocates and professionals should be consulted where appropriate.

Any information shared must be limited to what is necessary, relevant and proportionate. The capacity assessment, best-interests decision, information-sharing decision and reasons must be recorded.

A lack of capacity does not remove the person's rights under data protection law or the duty to protect their confidentiality. Information may nevertheless be shared without consent where another lawful and justifiable basis applies, including safeguarding, legal obligation, prevention of serious harm or individual care.

5.11 Anonymisation and Pseudonymisation Considerations

Anonymisation

Anonymisation is the process of changing personal information so that individuals are no longer identifiable by Abbeyfield Tamar Extra Care Society or by another person using means reasonably likely to be available.

Removing a name, address or other direct identifier will not necessarily anonymise information. Staff must also consider whether a person could be identified through reference numbers, dates, locations, rare characteristics, small numbers, combinations of information or information available from another source.

Information that has been effectively anonymised is no longer personal data for the purposes of UK data protection law. However, it must still be handled appropriately where it remains confidential, commercially sensitive or subject to another legal or contractual restriction. information is not necessary for the intended purpose. The effectiveness of the anonymisation and the risk of re-identification must be assessed before the information is used or disclosed.

Pseudonymisation

Pseudonymisation is the processing of personal information so that it cannot be attributed to a specific person without the use of additional information, such as a code or re- identification key. The additional information must be kept separately and protected by appropriate technical and organisational measures.

Pseudonymised information remains personal data where Abbeyfield Tamar Extra Care Society, its processor, a joint controller or another relevant party can use additional information to identify the person. It remains subject to applicable data protection, confidentiality and security requirements.

The re-identification key must only be accessible to specifically authorised people and must not be stored with the pseudonymised information. Pseudonymisation reduces risk but does not provide the same protection as effective anonymisation.

Further information can be found in the current Information Commissioner's Office guidance on anonymisation, pseudonymisation and data sharing.

5.12 Abbeyfield Tamar Extra Care Society Confidentiality

Suppliers

Staff must apply appropriate confidentiality and security controls when handling commercially sensitive, operational or proprietary information belonging to Abbeyfield Tamar Extra Care Society or another organisation.

Before appointing a software vendor or another supplier that will process personal information, Abbeyfield Tamar Extra Care Society will establish the data protection roles and responsibilities of the parties and complete proportionate due diligence covering privacy, confidentiality, information security, resilience, incident management and deletion or return of information.

Where a supplier acts as a data processor, an appropriate written contract meeting the applicable requirements of UK data protection law must be in place before processing begins. The processor must only act on documented instructions from Abbeyfield Tamar Extra Care Society, maintain appropriate security, support the exercise of individual rights, report personal data breaches without undue delay and obtain authorisation before appointing a sub-processor.

Any applicable requirements relating to international data transfers, data location, business continuity, system availability, audit, termination and secure data return or deletion must also be addressed.

Staff and external suppliers must not disclose confidential information such as supplier prices, performance, costs, security arrangements or contractual information to another supplier or unauthorised person unless the disclosure is authorised, required by law or otherwise justified.

An appropriate confidentiality agreement or confidentiality clause must be in place where a supplier will receive confidential information belonging to Abbeyfield Tamar Extra Care Society, the Service User / Residents, member of staff or another party. This does not replace the requirement for a data processing contract where the supplier acts as a processor.

Questions about the handling or disclosure of commercially sensitive information must be discussed with Registered Manager or another appropriately authorised person.

Meetings

Confidential information must only be discussed at a meeting where this is necessary for the purpose of the meeting and only with people who are authorised to receive it.

Meeting invitations, agendas, papers, attendance records, minutes, recordings and follow- up correspondence must be created, shared, stored and disposed of securely. Records of meetings containing personal information must be accurate, relevant and retained in accordance with the applicable retention arrangements.

Virtual or hybrid meetings must use approved systems. Staff must consider the privacy of the location, verify participants where necessary and prevent unauthorised people from seeing, hearing or recording the discussion.

Meetings must not be photographed, audio-recorded, video-recorded, transcribed by an automated tool or processed through an artificial intelligence system unless this has been specifically authorised and the relevant data protection and confidentiality requirements have been addressed.

Where the Freedom of Information Act 2000 applies to Abbeyfield Tamar Extra Care Society or to information held on behalf of a public authority, requests and disclosure decisions must be managed through the appropriate Freedom of Information procedure.

Complaints and Investigations

Complaints, concerns, disciplinary matters and investigations must be handled sensitively and confidentially. Information must only be accessed or shared by people who require it to receive, assess, investigate, respond to or oversee the matter.

Information may be disclosed where this is necessary for a fair investigation, safeguarding, legal advice, insurance, regulatory reporting, law enforcement, a court process or another lawful and justified purpose. Only the minimum necessary information must be disclosed.

Confidentiality must not be used to prevent a person from raising a safeguarding concern, making a protected disclosure, reporting wrongdoing, cooperating with a regulator or exercising another legal right.

Media

Staff must not disclose confidential information or make comments to the press, social media or other media on behalf of Abbeyfield Tamar Extra Care Society unless authorised to do so. Media enquiries must be referred to the person responsible for handling them.

Nothing in this section prevents a member of staff from making a lawful protected disclosure or reporting a concern through an appropriate authorised route.

5.13 Confidentiality Breach

A confidentiality or personal data breach may involve the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal or confidential information. Examples include misdirected correspondence, inappropriate access to a care record, loss of a device, disclosure to an unauthorised person,

cyberattack, insecure disposal, unauthorised screenshots or disclosure to an unapproved artificial intelligence system.

A breach may contravene data protection law, the common law duty of confidentiality, professional requirements or the policies of Abbeyfield Tamar Extra Care Society and may result in disciplinary, regulatory, contractual or legal action.

Any actual or suspected confidentiality, personal data or information security breach must be reported immediately to Registered Manager using the approved incident-reporting process. Staff must not wait until the full facts are known before reporting the incident.

Immediate steps must be taken, where safe and appropriate, to contain the breach and reduce harm. Staff must preserve relevant evidence and must not delete records, messages or system information that may be required for the investigation.

All actual or suspected personal data breaches must be escalated without undue delay to Business Manager or the person responsible for data protection so that the nature, scope, affected information, potential consequences and risk to individuals can be assessed.

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, Abbeyfield Tamar Extra Care Society must notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

Where the breach is likely to result in a high risk to affected individuals, they must also be informed without undue delay unless a lawful exception applies.

The need to notify commissioners, safeguarding bodies, professional regulators, insurers, law enforcement, the Care Quality Commission, NHS England or another relevant body must also be considered where applicable.

All personal data breaches must be documented, including those that do not meet the threshold for notification to the Information Commissioner's Office. The record must include the facts of the breach, its effects, the risk assessment, containment measures, decisions about notification and remedial action.

Breaches and near misses will be monitored by Registered Manager. Investigations will identify contributing factors, remedial action and lessons learned. Themes, repeated incidents and completion of actions will form part of the quality assurance programme for

Staff will refer affected people to the Complaints, Suggestions and Compliments Policy and Procedure and the relevant data protection complaints procedure at Abbeyfield Tamar Extra Care Society. Providing access to a complaints process does not replace the requirement to assess whether the person must be informed directly about a breach.

5.14 The National Cyber Security Centre

The National Cyber Security Centre provides guidance to help organisations reduce the risk of common cyberattacks. Abbeyfield Tamar Extra Care Society will have regard to relevant National Cyber Security Centre guidance, including the following areas: Step 1: Backing up important data and testing that it can be restored Step 2: Protecting devices, systems and information from malware Step 3: Keeping smartphones, tablets and other devices secure

Step 4: Protecting accounts through appropriate authentication, including multifactor authentication or passkeys where available Step 5: Recognising, reporting and responding to phishing and other attempted scams resources, including the Cyber Action Plan and current guidance linked in the Underpinning Knowledge section.

National Cyber Security Centre guidance supports but does not replace the need for organisation-specific cybersecurity policies, risk assessments, access controls, software updates, incident-response arrangements, tested backups, business continuity plans, staff training and supplier assurance.

Where applicable, Abbeyfield Tamar Extra Care Society must also meet relevant requirements of the Data Security and Protection Toolkit and the National Data Guardian's data security standards.

Staff must report suspected phishing, malware, ransomware, account compromise, unauthorised system access or other cyber incidents immediately through the approved incident-reporting route.

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

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 Criminal Record

A record of convictions held on the Police National Computer (PNC) for individuals convicted of crimes (includes information on cautions, reprimands, final warnings and bind-overs)

6.8 Business Sensitive information

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

6.9 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

6.10 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 / Residents information across the NHS and social care safely, efficiently and accurately

6.11 Confidentiality

Confidentiality means that professionals should not tell other people personal things about a Service User / Residents unless the Service User / Residents says

they can, or if it is absolutely necessary

6.12 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

6.13 Personal Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data Personal data breaches include incidents that are the result of both accidents (such as sending an email to the wrong recipient) as well as deliberate acts (such as phishing attacks to gain access to customer data) A personal data breach is a security incident that negatively impacts the confidentiality, integrity, or availability of personal data

6.14 AI

AI means Artificial Intelligence which is an umbrella term for a range of algorithm- based technologies that solve complex tasks by carrying out functions that previously required human thinking

6.15 Consent (CQC)

A person's voluntary agreement to a proposed action, particularly in relation to care, treatment, or support

7. Key Facts - Professionals

Professionals providing this service should be aware of the following:

Personal and confidential information must only be accessed, used or shared for a clear and legitimate purpose and where there is an appropriate lawful and justifiable basis Consent is not always required. Information may be shared without consent where this is necessary and justified for individual care, safeguarding, compliance with a legal obligation or court order, prevention of serious harm or serious crime, or another overriding public interest A lawful basis under data protection law does not, by itself, remove the common law duty of confidentiality. Where confidential information is involved, professionals must also establish consent, implied consent within the person’s reasonable expectations for individual care, a legal requirement or another justifiable basis for disclosure When the Service User / Residents dies, the duty of confidentiality may continue even though the UK GDPR and Data Protection Act 2018 do not apply to information relating to deceased people. Other legal restrictions may also apply

Information sharing must be necessary, proportionate, relevant, accurate, timely and secure. Only the minimum information required for the identified purpose should be shared, and only with appropriately authorised people who need it The identity and authority of the recipient must be verified before confidential information is shared A decision to share or not to share information must be recorded, including the reason, what was shared, with whom and for what purpose Family members, friends, carers and nominated contacts do not have an automatic right to receive confidential information. Their authority or another appropriate basis for sharing must be established Where a person lacks capacity to make the relevant decision, professionals must follow the Mental Capacity and Best Interests policies and procedures. A relative or carer does not automatically have authority to consent on the person's behalf Personal or confidential information must not be entered into an unauthorised artificial intelligence system or stored, photographed, copied or transmitted using an unauthorised personal device, email account, messaging application or cloud service Actual or suspected confidentiality, personal data or cyber security incidents must be reported immediately through the approved incident-reporting process Where there is doubt, advice must be sought from Registered Manager, the Data Protection Officer, Caldicott Guardian, safeguarding lead or another appropriately authorised person. Urgent and necessary information sharing must not be delayed where action is required to prevent serious harm

8. Key Facts - People Affected by The Service

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

You have the right to expect that information about you will be treated confidentially, protected securely and only accessed, used or shared for an appropriate purpose Staff will ask for your consent where consent is the appropriate basis for sharing information. However, consent is not always required Staff will normally explain how and why your information is used and shared. There may be circumstances where they cannot tell you in advance, for example where doing so would place someone at risk or prejudice an investigation If there is reason to believe that you may be unable to make a particular decision, staff will support you to make the decision for yourself wherever possible. If you lack capacity to make that decision, staff will follow the Mental Capacity Act 2005, its Code of Practice and the Mental Capacity and Best Interests policies and procedures Your family, friends and carers will not automatically be given information about you. Information may be shared with them where you agree, where they have lawful authority or where there is another appropriate reason You can express your views or object to information being shared. Staff must consider and record your wishes, although an objection will not always prevent sharing where there is another lawful and justified reason You may ask to see the personal information held about you. You can make this request verbally or in writing. You should tell staff if information held about you is inaccurate or incomplete so that it can be reviewed

You can make a complaint if you are concerned about how your information has been accessed, used, protected or shared If a breach involving your information is likely to create a high risk to you, Abbeyfield Tamar Extra Care Society will normally inform you without undue delay and explain the steps being taken

Further Reading

GOV.UK - Information: To Share or Not to Share, The Information Governance

Review (Historical Reference):
https://www.gov.uk/government/publications/the-information-governance-review

National Data Guardian - The Caldicott Principles:
https://www.gov.uk/government/publications/the-caldicott-principles

Care Quality Commission - Using Surveillance in Your Care Service:
https://www.cqc.org.uk/guidance-providers/all-services/using-surveillance-your-care-service

Information Commissioner's Office - Anonymisation and Pseudonymisation:
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data- sharing/anonymisation/

Information Commissioner's Office - Information for the Public About Personal

Information and Data Protection Rights:
https://ico.org.uk/for-the-public/

UK Caldicott Guardian Council:
https://www.gov.uk/government/groups/uk-caldicott-guardian-council

Information Commissioner's Office - Data (Use and Access) Act 2025:
https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act- 2025/

Information Commissioner's Office - How to Deal with Data Protection Complaints:

https://ico.org.uk/for-organisations/how-to-deal-with-data-protection-complaints/

Information Commissioner's Office - Special Category Data:
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special- category-data/

Information Commissioner's Office - Individual Rights:
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual- rights/individual-rights/

Information Commissioner's Office - Artificial Intelligence and Data Protection:

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/

Information Commissioner's Office - Personal Data Breaches:
https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

National Cyber Security Centre - Small Organisations Guide to Cyber Security:
https://www.ncsc.gov.uk/collection/small-organisations-guide-to-cyber-security

Additional Policies and Procedures

This policy must be read alongside the relevant policies and procedures available within Data protection impact assessments Data breaches and incident reporting Complaints, suggestions and compliments Safeguarding adults and children Mental capacity and best-interests decision-making Information security and cybersecurity

Outstanding Practice

To be "outstanding" in this policy area you could provide evidence that:
The revised policy is proactively communicated through the QCS App and other appropriate methods, with evidence that relevant staff have read, understood and can apply it in practice Effective governance, access controls, monitoring and audit arrangements protect staff and Service User / Residents confidentiality and identify potential weaknesses, inappropriate access or repeated incidents Staff can demonstrate how privacy, dignity and confidentiality are protected during personal care, conversations, record keeping, remote communication and the use of technology Each person's privacy, communication needs and reasonable expectations about the use and sharing of their information are identified, recorded, reviewed and met as far as reasonably possible Staff treat Service User / Residentss with kindness and respect and can explain how they protect confidentiality while sharing information appropriately for safe care and safeguarding Staff receive role-appropriate information governance and cyber security training, with competency assessed through supervision, scenarios, audit or observation rather than attendance alone Access to electronic care records is reviewed and audited, with unexplained or inappropriate access investigated Information-sharing decisions are well-documented and audits demonstrate that staff neither share information inappropriately nor withhold information needed for

safe care or safeguarding Data protection impact assessments are completed and reviewed for new or significantly changed technologies, surveillance, monitoring and artificial intelligence systems where required Personal data breaches, cyber incidents and near misses are analysed for themes, with evidence that learning results in completed and effective improvements People receive clear and accessible information about how their information is used and can explain how to exercise their rights or make a complaint Suppliers processing personal information are subject to proportionate due diligence, contractual controls and ongoing assurance Business continuity and downtime arrangements are tested to ensure that authorised staff can access clinically important information when needed Staff understand that public or unauthorised artificial intelligence tools must not be used to process personal or confidential information Leaders can demonstrate effective oversight of information governance risks, complaints, breaches, access audits, staff training, supplier assurance and improvement actions

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
Data Security Guidance - CR07	To detail the requirements for safe and secure records management.	QCS

Staff Confidentiality Agreement - CR07

This agreement is provided to clarify the responsibilities of those employed at information gathered by the service in the course of its work.

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

the:

Registered Manager

Registered Manager 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 Abbeyfield Tamar Extra Care Society 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 / Residents.

In the course of your work at Abbeyfield Tamar Extra Care Society, 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 Abbeyfield Tamar Extra Care Society

Associated health and social care professionals

Unless acting on practice policy or following the direct instructions of Abbeyfield Tamar Extra Care, or the Registered Manager, 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 Abbeyfield Tamar Extra Care Society, you must ensure that all records, including computer screens and computer-generated records or paper records of staff or Service User / Residents 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 Abbeyfield Tamar Extra Care Society 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 Abbeyfield Tamar Extra

Care Society. 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:

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 / Residents'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 Abbeyfield Tamar Extra Care Society, 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 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 Abbeyfield Tamar Extra Care Society should not be used to transfer commercially sensitive or personal identifiable information outside of 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 Abbeyfield Tamar Extra Care Society 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 / Residents/person identifiable information without the consent of the Service User / Residents'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.