Proxycare Personnel Ltd

Confidentiality Policy (England Community)

Regulatory Links

- **Health and Social Care Act 2008 (Regulated Activities) Regulations 2014**
- Regulation 17: Good governance – systems must be in place to maintain confidentiality of personal information
- Regulation 10: Dignity and respect – includes maintaining privacy and confidentiality
- Regulation 12: Safe care and treatment – confidential information sharing to ensure safety
- Regulation 13: Safeguarding service users from abuse and improper treatment – appropriate information sharing
- Regulation 18: Staffing – staff must be trained in confidentiality requirements
- **CQC Quality Statements**
- Safe systems, pathways and transitions (QS2): "We work with people and our partners to establish and maintain safe systems of care, in which safety is managed, monitored and assured. We ensure continuity of care, including when people move between different services."
- Treating people as individuals (QS16): "We treat people as individuals and make sure their care, support and treatment meets their needs and preferences. We take account of their strengths, abilities, aspirations, culture and unique backgrounds and protected characteristics."
- Independence, choice and control (QS17): "We promote people's independence, so they know their rights and have choice and control over their own care, treatment and wellbeing."
- Governance, management and sustainability (QS31): "We have clear responsibilities, roles, systems of accountability and good governance. We use these to manage and deliver good quality, sustainable care, treatment and support. We act on the best information about risk, performance and outcomes, and we share this securely with others when appropriate."

Scope

This policy applies to:

- All staff, including permanent, temporary, bank, and agency workers
- Volunteers and students on placement
- Contractors and third parties who have access to personal information
- All services we provide, including domiciliary care, supported living, and residential care
- All personal information about people we support, their families, staff, and business contacts

This policy applies to information in all formats, whether paper-based, electronic, verbal, or visual (such as photographs). It covers information accessed on organisation premises, in people's homes, remotely, or via mobile devices.
This policy should be read alongside our Data Protection Policy, Record Keeping Policy, Data Security Policy, Safeguarding Adults Policy, and Whistleblowing Policy.

Equality Statement

Our organisation is committed to equal rights and the promotion of choice, person-centred care and independence. This policy demonstrates our commitment to creating a positive culture of respect for all individuals. The intention is, as required by the Equality Act 2010, to identify, remove or minimise discriminatory practice in the nine named protected characteristics of age, disability, sex, gender reassignment, pregnancy and maternity, race, sexual orientation, religion or belief, and marriage and civil partnership. It is also intended to reflect the Human Rights Act 1998 to promote positive practice and value the diversity of all individuals.

Policy Statement

We are committed to protecting the confidentiality of everyone connected with our service. The people we support trust us with sensitive personal information about their health, relationships, finances, and daily lives. Protecting this information is fundamental to good care and maintaining trust.
Confidentiality is a legal requirement under the Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR). It is also an ethical duty central to professional care practice. Breaching confidentiality can cause real harm to individuals and may result in regulatory action, legal consequences, and damage to our reputation.
This policy sets out what confidentiality means in practice, when information can and should be shared, and what staff must do to keep personal information safe. We recognise that good information sharing is essential for safe, effective care, and this policy provides clear guidance on how to share information appropriately while maintaining confidentiality.

Policy Detail

What Confidentiality Means

Confidentiality means keeping personal information private and only sharing it with people who have a legitimate need to know. In care settings, this includes information about:

- Health conditions, diagnoses, and treatments
- Personal care needs and preferences
- Medical history and medications
- Mental health information
- Family circumstances and relationships

- Financial information
- Religious and cultural beliefs
- Sexual orientation and gender identity
- Contact details and addresses
- Information about safeguarding concerns

Confidentiality also extends to staff personal information, business-sensitive data, and any other information that is not meant to be public.

The Legal Framework

Several laws govern how we handle confidential information:

Data Protection Act 2018 and UK GDPR

These laws set out strict rules for processing personal data. Personal data means any information that can identify a living person. Special category data (such as health information, ethnicity, or sexual orientation) has additional protections. We must have a lawful basis for processing personal data and must only collect what we need for a specific purpose.

Common Law Duty of Confidentiality

Beyond data protection law, there is a common law duty of confidentiality. When someone shares personal information in circumstances where they expect it to be kept private, we have a duty not to disclose that information without their consent, unless there is a lawful basis for doing so.

Human Rights Act 1998

Article 8 protects the right to respect for private and family life, home, and correspondence. This underpins our duty to protect personal information and only share it when justified.

Caldicott Principles

Although not legislation, the Caldicott Principles provide important guidance on handling patient and service user information. These include: justify the purpose; don't use more information than necessary; use the minimum necessary; access should be on a strict need-to-know basis; everyone must understand their responsibilities; and the duty to share can be as important as the duty to protect.

When We Can Share Information

Information can be shared when:

- The person has given consent: The person (or someone with legal authority to consent on their behalf) has agreed to the information being shared. Consent should be informed, specific, and freely given.
- It is necessary for their care: Sharing is needed to provide or coordinate care and treatment. Staff involved in someone's care need access to relevant information to do their job safely.
- There is a safeguarding concern: If someone is at risk of abuse, neglect, or harm, we may need to share information without consent to protect them or others. This should be proportionate and involve only the information necessary.
- There is a legal requirement: Some legislation requires us to share information, for example, notifying CQC of certain incidents, or responding to court orders.

- There is an overriding public interest: In rare cases, sharing may be justified in the public interest, such as preventing serious crime or protecting public health.

When sharing without consent, we will document the decision-making process, including who made the decision and why. We will share only the minimum information necessary and inform the person about the disclosure where possible and safe to do so.

The Duty to Share Information

Confidentiality is not about keeping secrets or refusing to share any information. There is an equally important duty to share information when it is necessary to protect people or provide safe care. Many serious case reviews have identified failures to share information as a contributing factor in harm coming to vulnerable people. Staff should never use "confidentiality" as a reason not to share information that is needed to safeguard someone or coordinate their care.
The key principles are:

- Share with the right people, for the right reasons, at the right time
- Share the minimum information needed for the purpose
- Be transparent with the person about what you are sharing and why, unless this would increase risk
- Record what you shared, with whom, and why
- Seek advice from your manager or safeguarding lead if you are unsure

Staff Responsibilities

All staff must:

- Complete confidentiality training during induction and refresher training as required
- Only access information that they need to do their job
- Never share their passwords or allow others to use their login credentials
- Keep written records secure and out of sight of unauthorised people
- Be aware of their surroundings when discussing confidential matters
- Never discuss people we support in public places where they may be overheard
- Never share information about people we support on social media or messaging apps
- Report any breaches or suspected breaches immediately
- Maintain confidentiality even after leaving employment with us

Handling Requests for Information

Staff may receive requests for information from various sources. The response depends on who is asking and why.

Requests from family members or friends

Do not assume that family members have a right to information about an adult we support. Always check whether consent has been given or whether the person is recorded as a nominated contact in the care plan. If in doubt, politely explain that you need to check and speak to your manager.

Requests from other professionals

Verify the identity and role of anyone claiming to be a professional before sharing information. Check that they have a legitimate need for the information and that sharing is in the person's interests or required for their care. Record who you shared information with and why.

Requests from the police or other authorities

These requests should be escalated to a manager. We may share information with police if there is consent, a court order, or an urgent safeguarding need. Routine requests should be made formally and in writing. Record all such requests and responses.

Subject access requests

People have a legal right to access their personal data under UK GDPR. These requests must be responded to within one month. All subject access requests should be passed immediately to the Registered Manager or Data Protection Lead.

Protecting Information in Practice

In offices and care settings

- Lock cabinets and drawers containing personal information when not in use
- Position computer screens so they cannot be seen by visitors or unauthorised people
- Use privacy screens on monitors where appropriate
- Lock or log off computers when leaving them unattended
- Dispose of confidential paper records using confidential waste bins or shredding
- Hold confidential conversations in private spaces, not corridors or reception areas

When visiting people in their homes

- Keep care records secure and out of sight during visits
- Do not leave documents visible in your car
- Be mindful of others in the home who may overhear conversations
- Return any documents to secure storage at the end of your shift
- If using a personal device for work purposes, ensure it is password-protected and encrypted

Electronic communications

- Use only approved systems and devices for work communications
- Check email addresses carefully before sending sensitive information
- Use encryption or secure file transfer for sensitive documents
- Never share personal information about people we support via personal email, WhatsApp, or social media
- Report any suspected phishing attempts or security incidents immediately
- When emailing health and social care organisations, use systems that meet the secure email standard (DCB1596) to ensure sensitive information is protected in transit
- To reduce the risk of misdirected emails, copy and paste email addresses from a recorded source rather than typing them manually, and consider sending a test email before transmitting sensitive information

Conversations and Verbal Information

Confidentiality applies to spoken information just as much as written records. Staff must be careful about where and how they discuss confidential matters.

- Never discuss people we support by name in public places such as cafes, shops, or public transport
- Be aware that conversations in offices or staff rooms may be overheard
- Keep telephone conversations private and be aware of who is nearby
- Do not take phone calls about work matters in front of other people we support or their visitors
- In handovers, only share information that the next staff member needs to know

Social Media and Personal Devices

Social media poses particular risks to confidentiality. Staff must:

- Never post photographs of people we support on personal social media accounts
- Never identify people we support by name, location, or any other detail that could identify them
- Not discuss work, people we support, or colleagues on social media
- Not accept friend requests from people we support or their families on personal social media
- Be aware that even vague references can breach confidentiality if they allow identification

Personal mobile phones should not be used to take photographs in care settings unless there is explicit consent and a legitimate work purpose, and this has been authorised by a manager.

Mental Capacity and Confidentiality

The Mental Capacity Act 2005 is relevant when sharing information about someone who may lack capacity to consent to disclosure.

- Always assume capacity unless there is evidence to suggest otherwise
- Capacity is decision-specific. Someone may have capacity to consent to some disclosures but not others
- Where someone lacks capacity, decisions about sharing their information must be made in their best interests
- Consider whether there is a Lasting Power of Attorney for Health and Welfare in place, and if so, whether the appointed attorney should be consulted about the disclosure
- Record mental capacity assessments and best interests decisions about information sharing

Confidentiality After Death

The duty of confidentiality does not end when someone dies. Staff must continue to protect personal information about people we have supported after their death. Information should only be shared where there is a lawful basis, such as for registering the death, supporting a coroner's

investigation, or with the consent of the personal representative of the deceased. Staff should refer to our End of Life Policy for further guidance on handling information after someone has died.

Confidentiality Breaches

A breach occurs when confidential information is accessed, shared, or lost inappropriately. This includes:

- Sharing information with someone who does not have a right or need to know
- Leaving documents where they can be seen by unauthorised people
- Losing paper records or electronic devices containing personal information
- Sending information to the wrong person
- Accessing records out of curiosity rather than for a work purpose
- Discussing identifiable information in an inappropriate setting

All breaches must be reported immediately to the Registered Manager. Serious breaches may need to be reported to the Information Commissioner's Office within 72 hours. Breaches will be investigated, with initial findings documented within 14 days. Investigations may result in disciplinary action up to and including dismissal. Serious breaches may also lead to criminal prosecution or regulatory action.

Registered Professionals

Some staff may be registered with professional bodies that set additional standards for confidentiality. Where our organisation employs or works with registered professionals, those individuals must comply with both this policy and the requirements of their professional regulator. Registered nurses and nursing associates are bound by the Nursing and Midwifery Council (NMC) Code, which requires them to respect people's right to privacy and confidentiality. This includes ensuring that people are informed about how their information is used and shared, sharing information only when the interests of safety and public protection override the need for confidentiality, and recognising that the duty of confidentiality continues after someone has died. Breaches of confidentiality by registered nurses may result in fitness to practise proceedings in addition to any internal disciplinary action.

All staff, whether or not they are registered professionals, should be aware that the principles of confidentiality in professional codes closely align with this policy. The Skills for Care Code of Conduct for Healthcare Support Workers and Adult Social Care Workers in England also sets clear expectations about treating information confidentially and only disclosing it in accordance with legislation and agreed ways of working.

Training Requirements

All staff will receive training on confidentiality as part of their induction. This will cover:

- The legal framework for confidentiality and data protection
- Practical measures for protecting information
- When and how information can be shared
- Recognising and reporting breaches
- Using systems and devices securely

Refresher training will be provided at least every two years, or sooner if there are significant changes to legislation or practice. Understanding of confidentiality requirements will be checked through supervision and competency assessments.

Procedures

Responding to Requests for Information

- When someone asks for information about a person we support, ask who they are and why they need the information.
- Verify their identity. For telephone callers, consider calling back on a number you have on record.
- Check the care plan to see whether the person has consented to information being shared with this individual.
- If consent is recorded, share only the information needed for the stated purpose.
- If consent is not recorded, politely explain that you need to check and will get back to them. Speak to your manager.
- Record the request and your response in the person's records.
- If you are unsure whether to share information, do not share it until you have sought guidance.

Sharing Information for Safeguarding

- If you have a safeguarding concern that requires information sharing without consent, speak to the Safeguarding Lead or Registered Manager immediately.
- Explain what information you think needs to be shared and why.
- The manager will decide whether sharing is necessary and proportionate.
- If sharing is agreed, share only the information needed to address the safeguarding concern.
- Record the decision, the rationale, what was shared, and with whom.
- Where possible and safe, inform the person that information has been shared and why.
- If the person is upset about the disclosure, listen to their concerns and explain the reasons again.

Reporting a Confidentiality Breach

- As soon as you become aware of a breach or potential breach, report it to the Registered Manager or senior manager on duty.
- If the breach involves electronic systems, also notify the IT lead or Data Protection Lead.
- Provide as much detail as possible: what happened, when, what information was involved, and how many people may be affected.
- Take immediate steps to contain the breach if possible, such as retrieving misdirected documents.

- The manager will assess the severity and decide whether notification to the Information Commissioner's Office is required.
- The manager will also decide whether affected individuals need to be informed.
- Complete an incident report within 24 hours.
- Cooperate fully with any investigation into the breach.

Handling Subject Access Requests

- If someone asks to see the personal information we hold about them, this is a subject access request.
- Pass the request immediately to the Registered Manager or Data Protection Lead.
- Verify the identity of the person making the request.
- The Data Protection Lead will coordinate the response, gathering relevant records.
- Information about third parties may need to be redacted before disclosure.
- The response must be provided within one calendar month of the request.
- Record the request and the response.

Secure Disposal of Confidential Information

- Never put confidential documents in normal waste bins or recycling.
- Use designated confidential waste bins or shred documents using a cross-cut shredder.
- Confidential waste bins must be kept locked and emptied by an approved confidential waste contractor.
- Electronic devices must be wiped or destroyed according to our IT disposal procedures before being discarded or recycled.
- Obtain certificates of destruction where appropriate.

Records must be retained in accordance with our Record Keeping Policy and retention schedule before being disposed of. Health and care records for adults are typically retained for eight years after the last contact, but some records require longer retention.

Staff Leaving Employment

- Return all documents, equipment, and devices containing personal or confidential information.
- Delete any work-related information from personal devices if previously authorised to hold it.
- Hand in ID badges, keys, and access cards.
- System access will be revoked on or before the last day of employment.
- The duty of confidentiality continues after employment ends. Former staff must not disclose confidential information obtained during their employment.

Working Remotely or From Home

- Only use approved devices and secure connections (VPN where required) to access work systems.
- Ensure no one else in the household can see your screen or overhear confidential calls.
- Do not print confidential documents at home unless absolutely necessary and authorised.
- If you must print documents, store them securely and return or shred them as soon as they are no longer needed.
- Lock devices when not in use, even at home.
- Report any security concerns or incidents immediately.
- Domiciliary care staff must not access electronic care records on public Wi-Fi networks. Use mobile data or wait until you have a secure connection.
- If you need to make notes during a visit, use only authorised paper forms or devices, and ensure these are stored securely between visits.

Auditing and Monitoring Compliance

- Access to electronic records may be audited to check for inappropriate access.
- Spot checks will be carried out on physical security of records.
- Confidentiality will be discussed in staff supervisions.
- Training records will be monitored to ensure all staff are up to date.
- Any patterns of concern will be addressed through additional training or, where necessary, disciplinary procedures.

References and Further Reading

Legislation

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Human Rights Act 1998
- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- Care Act 2014
- Mental Capacity Act 2005
- Computer Misuse Act 1990
- Freedom of Information Act 2000 (if applicable to your organisation)

CQC Guidance

Regulation 17: Good governance – https://www.cqc.org.uk/guidance-providers/regulations/regulation-17-good-governance
Regulation 10: Dignity and respect – https://www.cqc.org.uk/guidance-providers/regulations/regulation-10-dignity-respect

Information Commissioner's Office

Guide to UK GDPR – https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/
Data sharing: a code of practice – https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/
Reporting a breach – https://ico.org.uk/for-organisations/report-a-breach/

Other Guidance

Caldicott Principles – https://www.gov.uk/government/publications/the-caldicott-principles
Information sharing: advice for practitioners – https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice
NHS Confidentiality Code of Practice – https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
Code of Conduct for Healthcare Support Workers and Adult Social Care Workers in England, Skills for Care – https://www.skillsforcare.org.uk/resources/documents/Developing-your-workforce/Code-of-Conduct.pdf
The Code: Professional standards of practice and behaviour for nurses, midwives and nursing associates, NMC – https://www.nmc.org.uk/standards/code/
Data Security and Protection Toolkit – https://www.dsptoolkit.nhs.uk/
Digital Care Hub (formerly Digital Social Care) – https://www.digitalcarehub.co.uk/
Secure email standard (DCB1596) – https://digital.nhs.uk/services/nhsmail/the-secure-email-standard

Related Organisational Policies

- Data Protection Policy
- Record Keeping Policy
- Data Security Policy
- Safeguarding Adults Policy
- Whistleblowing Policy
- Social Media Policy
- IT Acceptable Use Policy
- Mental Capacity Policy
- Complaints Policy
- End of Life Policy
- Data Quality Policy

Appendix: Quick Reference Guide – Confidentiality Dos and Don'ts

This quick reference guide summarises the key points from this policy. Keep it handy as a reminder of good practice.

✅ DO:

Protecting Information

- Lock filing cabinets and drawers containing personal information
- Log off or lock your computer when leaving it unattended, even briefly
- Position your screen so visitors cannot see it
- Use confidential waste bins or shredders for documents with personal information
- Keep care records secure and out of sight during home visits
- Return documents to secure storage at the end of your shift
- Use strong passwords and keep them private

Sharing Information

- Check consent before sharing information with family members or others
- Verify the identity of anyone requesting information
- Share only the minimum information needed for the purpose
- Record what you shared, with whom, and why
- Share information when it is needed to safeguard someone from harm
- Ask your manager if you are unsure whether to share

Conversations

- Hold confidential conversations in private spaces
- Be aware of who might overhear your phone calls
- Keep handovers focused on what the next person needs to know
- Think before you speak – is this the right place to discuss this?

Reporting

- Report any breach or suspected breach immediately
- Report lost or stolen devices, documents, or records straight away
- Complete your confidentiality training and keep it up to date
- Raise concerns if you see others not following confidentiality rules

❌ DON'T:

Accessing Information

- Access records unless you need to for your work
- Look at records out of curiosity – even for people you know
- Share your password or let others use your login
- Leave yourself logged in on shared computers

Sharing Information

- Assume family members have a right to information about an adult
- Give out information over the phone without checking who is calling
- Share more information than is needed
- Use "confidentiality" as a reason not to share information needed for safeguarding

- Send sensitive information by personal email or messaging apps

Conversations

- Discuss people we support by name in public places
- Talk about work in cafes, shops, on the bus, or anywhere you might be overheard
- Gossip about people we support, their families, or colleagues
- Have confidential phone conversations where others can hear

Social Media and Devices

- Post anything about people we support on social media – even without names
- Take photos in care settings on your personal phone without authorisation
- Accept friend requests from people we support or their families
- Discuss work, colleagues, or people we support online
- Leave documents visible in your car

Documents and Records

- Leave confidential documents on desks, printers, or in unlocked drawers
- Put confidential waste in normal bins
- Take records home unless authorised and necessary
- Print confidential documents and forget to collect them

Key Reminders

Situation	What to Do
Someone asks for information about a person we support	Check their identity, check consent in the care plan, share only what is needed, record what you shared
You are unsure whether to share information	Do not share until you have spoken to your manager
You have a safeguarding concern	Share relevant information with the Safeguarding Lead or manager – do not let confidentiality stop you protecting someone
You accidentally send information to the wrong person	Report it immediately to your manager – do not try to cover it up
You lose a document or device	Report it straight away to your manager – quick action can limit the damage
Someone wants to see their own records	Pass the request to your manager or Data Protection Lead immediately
You see a colleague not following confidentiality rules	Speak to them if appropriate, or report to your manager

Remember: If in doubt, don't give it out. Ask your manager before sharing information if you are unsure. It is always better to check than to make a mistake that could harm someone or breach

their trust.
But also remember: Sharing information appropriately is essential for safe care and safeguarding. Never use confidentiality as a reason not to share information that could protect someone from harm.