



Top 10 tips for care providers encountering everyday technology in people's homes

1. Be aware that conversations may be recorded

Ring doorbells, smart speakers and home cameras may capture audio as well as video. Conversations between staff and the person drawing on support, including discussions about medication, health, personal circumstances or care needs, could be picked up and stored.

- Look for visible cameras, doorbells, microphones and smart speakers.
- Be mindful of conversations within recording range, including doorstep conversations and speakerphone calls.
- Never assume a conversation is private just because you are inside someone's home.
- Where confidential discussions are needed, agree a more appropriate setting or ask whether the device can be muted, with the person's permission.

Remember: A device's presence does not necessarily mean it is recording continuously. Staff should understand the possible functions without making assumptions.

2. Have clear organisational policies and procedures

Providers should have policies that explicitly address everyday technology owned or installed by people receiving care and support. Staff need to know what is expected of them and how to respond consistently.

Policies should explain:

- How staff develop a broad understanding of common smart devices (IoT) and their possible recording, monitoring and information-sharing functions.

- How confidential conversations, care records, handovers and telephone calls should be managed.
- How to respond if a person asks staff to be recorded or shares footage with the provider.
- How to raise concerns about privacy, safeguarding, inappropriate use or staff conduct.
- Who to contact for advice, how incidents are documented and how concerns are escalated.

Policies should respect the person's ownership of their home and technology while setting clear expectations for professional practice. Staff should know where to find the guidance and how it applies to real situations.

3. Include everyday technology within the risk assessment process

Build consideration of personal technology into the provider's existing assessment and care planning processes, rather than treating it as an isolated IT issue.

Consider:

- Devices and capabilities: What is present, and can it capture audio, video, location or other personal information?
- Purpose and expected benefits: Why is the device used, what outcomes matter to the person, and how will you know whether it has helped?
- Privacy and confidentiality: Could conversations, care activities, medication details or information about other people be captured?
- Access and storage: Who may view recordings, receive alerts or access stored information?
- Safeguarding: Could the technology create risks of coercion, inappropriate monitoring, exploitation or unauthorised sharing?
- Practical controls and trial gateway: What steps would reduce the risks without unnecessarily restricting the person's independence? Where appropriate, use

a time-limited trial with agreed success criteria, support arrangements, an exit plan and a clear approval gateway before ongoing use.

Document the identified risks, expected benefits, agreed control measures, responsible people, trial decision and review arrangements. Revisit the assessment when circumstances change, the technology is updated or new concerns arise.

4. Provide staff training, guidance and ongoing support

Staff need more than a policy document. They should receive practical training and feel confident asking for advice when encountering unfamiliar technology.

Training should help staff:

- Recognise common devices and understand their potential recording, monitoring and data-sharing functions.
- Identify what information could be captured, including sensitive conversations and information about third parties.
- Contribute to risk assessments and recognise when a concern needs escalating.
- Apply practical controls, such as moving confidential discussions, using approved communication channels and protecting care records.
- Respond calmly and respectfully if a person explains that a conversation has been recorded.

Use realistic scenarios, such as a Ring doorbell recording a medication discussion, an indoor camera capturing a care visit, or a smart speaker activating during a handover. Provide refresher training, supervision and access to a manager or information governance lead when staff are unsure.

5. Talk openly and respectfully with the person

Approach conversations openly and without judgement.

- Ask how the technology works without implying the person has done anything wrong.
- Explain concerns clearly and listen to why the person uses the device.

- Agree practical arrangements wherever possible.

Example: "I noticed your doorbell has an audio function. Could we talk about how it works, so we can make sure any confidential care discussions are handled appropriately?"

6. Protect confidential information and professional boundaries

Protect confidential information and maintain professional boundaries.

- Avoid discussing identifiable information about other people within recording range. Treat smart technology like another person in the room: would you have the same conversation in front of a visitor or family member?
- Take care with handovers, telephone calls, electronic care records and sensitive conversations.
- Use approved systems and lock work devices when unattended.

7. Consider the rights and privacy of everyone affected

Balance the person's independence with the rights and privacy of others.

- Consider care workers, relatives, visitors, neighbours and other professionals who may be captured.
- Recognise the person's right to use their own smart technology, while considering the privacy and rights of everyone affected.
- Seek advice when the legal position is unclear.

8. Know how to respond to concerns or incidents

Follow organisational procedures when a genuine concern arises.

- Record factual observations and report concerns promptly.
- Involve the appropriate manager, safeguarding lead, Data Protection Officer or information governance lead.
- Do not access, delete or obtain recordings without appropriate authority.
- Distinguish ordinary use of technology from a concern that requires investigation.

9. Understand the technology without taking control of it

Staff should understand the general purpose and capabilities of common smart technology, without needing specialist technical knowledge or taking control of the person's devices.

- Recognise motion activation, audio recording, cloud storage, remote viewing and account access.
- Do not unplug, disable, cover or change settings without permission or authority.
- Discuss concerns with the person and seek advice.
- Consider proportionate alternatives where a device creates a significant risk.

10. Review practice and learn from experience

Review practice regularly and learn from experience.

- Review policies, training and individual risk assessments regularly.
- Reassess after concerns, incidents, complaints or significant changes in circumstances.
- Use supervision, team discussions and feedback from people drawing on care and support to identify what worked, where support is needed and how practice should change.
- Maintain a proportionate central record of outcomes and benefits from technology implemented, including what did not work. Use anonymised learning and success stories to improve practice and provide evidence for commissioners and regulatory inspections, rather than creating unnecessary paperwork.

Key aim: Develop a consistent culture in which staff feel confident managing everyday technology while protecting the person's rights, dignity, independence and safety.