



## Top 10 tips for care providers implementing everyday technology with someone who draws on care and support

### 1. Start with the person, not the technology

**Start with the person's needs, wishes, capacity, independence and circumstances before recommending a device.**

- Explain what the device does and what information it collects – ensure they truly understand this.
- Clarify who can access the information and any potential risks.
- Co-produce the approach with the person at every stage: identify what matters to them, agree the expected benefits and measures of success, choose and test options together, and use technology to support their choices rather than unnecessarily restrict independence.

### 2. Complete a privacy and risk assessment

**Assess privacy and risk before introducing the technology.**

- Identify all personal data collected, including health, location, audio, video and daily routines.
- Consider who genuinely needs access, grant only the permissions they need, and assess whether collection is necessary and proportionate (least privilege).
- Include hidden risks, such as care worker conversations being captured, and agree how these will be managed.
- Complete a Data Protection Impact Assessment (DPIA) where processing is likely to result in a high risk to people's rights and freedoms.

### 3. Support informed consent and respect the person's choices

**Explain the technology accessibly and respect the person's choices.**

- Check that the person understands the implications.

- Assess decision-making capacity where there is reason to doubt it, following the relevant legal framework.
- Distinguish consent to use a device, consent to share information and the lawful basis for processing data.
- If the person lacks capacity, follow legal and best-interests processes; a family member does not automatically have authority to consent.

#### 4. Check privacy settings before use

##### **Review privacy settings before the device is used.**

- Check app permissions and switch off unnecessary access, data collection, advertising personalisation, contact syncing and location sharing. For example, does a recording app really need access to contacts?
- Disable voice or video recording where it is not needed.
- Do not assume default settings are private.
- Use camera shutters, microphone mute buttons or privacy modes where available.

#### 5. Secure accounts, passwords and access

##### **Protect accounts and restrict access to authorised users.**

- Use unique passwords or passkeys and enable multi-factor authentication (MFA) where available.
- Change default credentials and give each authorised user their own account where possible.
- Avoid shared staff logins, insecure password lists and unnecessary administrator access.
- Remove access promptly when it is no longer needed.

#### 6. Keep devices and apps updated

##### **Keep devices and applications secure and supported.**

- Install security updates promptly and enable automatic updates where appropriate. Assign responsibility for monitoring and patching. Updates can fix security weaknesses, but may also introduce new features, including AI, or

change what information is collected, how it is used and whether it is processed offshore; review privacy and risk after material changes.

- Use supported devices and remove applications that are no longer needed.
- Before recommending a product, check how long the manufacturer will provide security updates and how it communicates material changes to features, data use and processing locations.
- Replace or reassess devices that no longer receive security patches.

## 7. Be careful about sharing information with families and professionals

**Share only the information each person genuinely needs.**

- Agree who needs access and what they need to see. Do not automatically give family members or professionals administrator access.
- Use limited alerts or reminders rather than unrestricted access where possible.
- Verify recipients before sharing information.
- Use secure channels and document the agreed arrangements.

## 8. Protect privacy and dignity in all care settings

**Protect dignity and privacy wherever care and support is provided.**

- Consider everyone who may be captured, including the person, visitors, neighbours and care workers.
- Review device placement, when recording occurs, who can view footage and how long it is retained.
- Avoid intrusive monitoring unless it is necessary, proportionate and legally justified.
- Be transparent with everyone affected where required.

## 9. Plan for incidents and technology failures

**Prepare staff and service users for incidents and technology failures.**

- Explain what to do if a device is lost, an account is compromised or a suspicious message is received.

- Provide a clear reporting route to the manager, IT lead or Data Protection Officer (DPO).
- Report accidental sharing of personal information promptly.
- Maintain backup arrangements where technology supports medication, falls alerts, safety or emergency communication.

## 10. Review, document and safely decommission

### **Document decisions, review arrangements and safe decommissioning.**

- Record why the technology was recommended, the person's goals and expected benefits, the assessment, trial and gateway decision, settings, authorised users, training and named owner.
- Co-produce reviews with the person and reassess when needs, wishes, software, firmware, suppliers, data use or processing locations change, or when new risks emerge. Confirm that the technology remains beneficial, proportionate and wanted.
- Remove accounts, permissions and access when a device is replaced or no longer required.
- Delete information where appropriate and securely reset or dispose of the device.