care inspectorate

Guidance for care providers in Scotland using CCTV (closed circuit television) in their services

HAPPY TO TRANSLATE®

This guidance draws on similar guidance produced by the Care Quality Commission (CQC) for use in England. We are grateful to the CQC for allowing us to use and adapt their 2015 guidance Using Surveillance: Information for Service Providers.

This Guidance is intended to provide general information about the use of surveillance in care service settings. It is not intended to be a statement of law and its contents do not form legal advice and it should not be acted on or relied on as such.

Please note that where the term "General Data Protection Regulation" is used throughout this guidance, this relates to the General Data Protection Regulation (Regulation (EU) 2016/679) and its incorporation into UK law, including the Data Protection Act 2018.

Rate this publication and tell us what you think with our short, four-question survey
surveymonkey.co.uk/r/rate-this-publication

Your views are helping us improve.

Contents

Introduction

This information is for providers of care services who may be considering using surveillance equipment such as CCTV cameras. It sets out some of the key points to consider and gives details of sources of further guidance and support.

If you are deciding whether to use surveillance in your service, you should do this in consultation with the people who use your service, appropriately involving families, carers, and staff before you install a system. How, and the extent to which, you do this will depend on the type of care you are providing and the type of surveillance you are considering. After you install a system all new families, carers and staff new to your service should be informed before they agree to join your service of the surveillance system in place. **This guidance does not tell you whether or not you should use surveillance systems and we do not require providers to use surveillance.**

Any use of surveillance in care services must be lawful, fair and proportionate, and used for purposes that support the delivery of safe, effective, compassionate and high-quality care. This is what the law requires and reflects the principles and details of new Health and Social Care Standards. If you already use surveillance, you should consider whether it was implemented, and is being used, with proper consideration of the issues raised in this document. If required, you should consider if you need to make changes to your surveillance methods.

We recognise that some providers may find significant benefits in using surveillance. In some cases, covert surveillance (such as hidden cameras or audio recording equipment) or overt surveillance (such as visible CCTV cameras) may be an effective way to ensure safety or help improve quality of care. We also recognise that there are growing assistive technologies other than CCTV, which are an important part of telecare and telehealth.

Before considering the use of CCTV it is essential that care providers recognise that there are other less intrusive steps they can take to ensure that care is high quality and safe.

- Always have enough capable and confident staff on duty who have the right mix of skills.
- Encourage an open culture, where both staff and people who use services are able to raise any concerns freely, knowing they will be addressed, including staff meetings, engagement with service users and carers, the promotion of independent advocacy and complaints procedures, as well as a clear whistleblowing policy.
- Ensure supervision and appraisal are used to develop and motivate staff and, where needed, review their practice or behaviour.
- Ensure people who experience care, families and carers are meaningfully involved in the service and regularly provide feedback on the care and support

We would be concerned if surveillance and the use of CCTV were routinely considered as a 'first step' and concerned about an over-reliance on surveillance to deliver key elements of care; it can never be a substitute for well-trained and well-supported staff.

If you are considering surveillance, particularly covert surveillance, you should bear in mind the potential impact on the bond of trust with people who use your service and the possible impact on employer/employee relationships. More guidance is provided below on the circumstances where you may consider covert surveillance.

CCTV and other types of cameras are the most obvious and high-profile surveillance technologies. However, not all surveillance involves cameras. For example, audio recording and transmitting equipment may also be used.

Any surveillance must comply with the law. Guidance provided here is designed to provide general information about your responsibilities but does not constitute legal advice and you should not treat it as such. Using surveillance in a lawful way is a complex topic and we suggest you consider obtaining expert legal advice when considering the use of surveillance, especially where it is likely to collect sensitive or special categories of personal information about people or intrude on their privacy. The examples in this guidance are general in nature and should not be assumed to apply to any specific situations.

Scotland's new Health and Social Care Standards, published in 2017, describe the outcomes people can expect when using social care services.

Standard 2.7 states that people can expect that:

"My rights are protected by ensuring that any surveillance or monitoring device that I or the organisation use is necessary and proportionate, and I am involved in deciding how it is used".

This should be an over-riding principle which providers should take account of when considering the use of any surveillance system.

Key points

CCTV use should not be 'first choice' and a default position, it does not substitute for having suitable numbers of competent staff and should only be used after full consideration of the alternatives and implications.

- Covert and overt surveillance can have legitimate uses. You should weigh their benefits against the impact on people's privacy, other issues set out in this guidance, and any relevant legislation, when deciding whether to use them.
- Surveillance in care services is likely to raise greater privacy concerns than in other kinds of business, especially where people also live in the place where the service is delivered.
- Wherever possible, you should consult with the people who use your service, their families and your staff when deciding whether and how to use surveillance.
- The Information Commissioner's Office guidance on privacy/data protection impact assessments is helpful.
- It is vital you work in a transparent and open way, to help comply with legal requirements and to maintain the trust of the people using your service and of your staff. However, there may be limited circumstances where the legitimate use of covert surveillance prevents such openness for a short time.
- You must ensure that all staff (including contractors) involved in the use of surveillance systems are properly trained and supported to use them.
- The equipment must be suitable, safe and properly maintained.
- Information obtained or recorded through the use of surveillance must be kept secure, and anyone with authorised access to that information must understand their legal responsibilities.
- Where people lack mental capacity to understand or consent to the use of surveillance, you must make decisions in accordance with the statutory principles of the Adults with Incapacity (Scotland) Act 2000 and the relevant sections of the Health and Social Care Standards (2.11 and 2.12).
- You should document the steps you have taken when deciding to use surveillance, as this evidence may be helpful to you or others later evaluating the way in which you provide care.

You must ensure that you and anyone acting on your behalf always comply with the Data Protection Act 2018, the General Data Protection Regulation and all other relevant legislation. Follow the guidance produced by the Information Commissioner's Office and, where relevant, the Surveillance Camera Commissioner, and seek expert legal advice where necessary.

Definitions

Surveillance is the monitoring of a place, person, group, or ongoing activity in order to gather information.

Overt surveillance is where the person being monitored would reasonably be aware of the surveillance. For example, visible CCTV cameras that are clearly signposted.

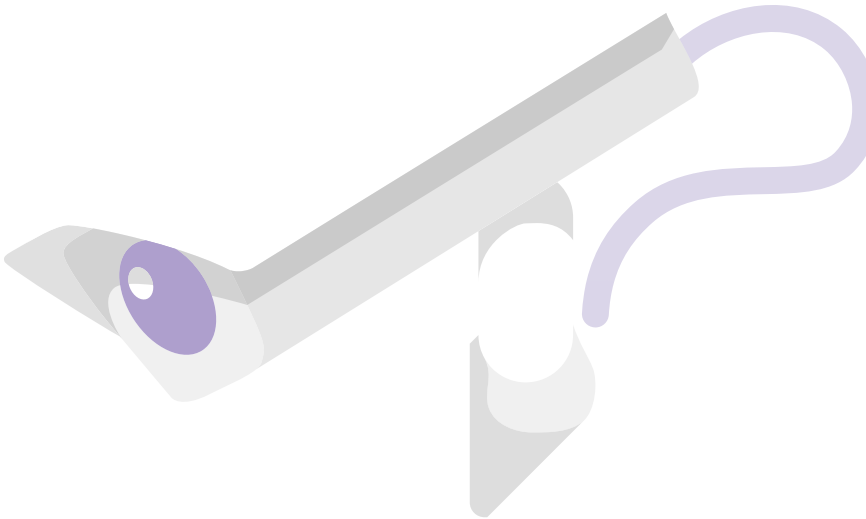
Covert surveillance is where the person being monitored would not reasonably be aware of the surveillance occurring. For example, hidden audio recording devices, used for a time-limited and specific purpose.

Surveillance systems are the technologies and equipment used to carry out surveillance or to store and process the information gathered. This encompasses CCTV, WiFi cameras, audio recording, radio-frequency identification (RFID) tracking and many other types of existing and emerging surveillance systems.

Privacy is the right of a person to be left alone, for example not to be observed or disturbed by others. Intrusion on privacy can include collecting information through surveillance or monitoring how people act in public or private spaces. The Information Commissioner's Office's Privacy Impact Assessment Code of Practice has more information about this.
https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

What this guidance does not cover

- Direct care assessment or treatment that gathers information. For example, equipment that monitors a person's vital signs, such as their heart rate, for medical or care purposes.
- Technology that is used with the knowledge and explicit consent of a person or their appropriate representative, specifically for the purpose of keeping a record of an episode of care or treatment.
- Communications systems controlled by the person using the service. For example, webcams that can be switched on and off by the user to contact the provider or alarm buttons that can be pressed in the event of a fall. This would not be considered as surveillance, but providers should still think about issues of privacy when using these systems.



1. Why might care providers want to use surveillance in their services?

The most common reasons surveillance systems such as CCTV are used are to keep premises and property secure and people safe. Surveillance may be used as an additional tool to help protect people from the risk of abuse, or to investigate allegations or serious concerns about possible abuse or potential criminality.

Surveillance systems may also be an effective way to promote and support independence and autonomy for people who use care services as part of a suite of assistive technology designed to monitor people's welfare with minimum restriction to their movements and activities.

2. Using surveillance lawfully and appropriately in care services

We consider the use of surveillance in a place where people are receiving care – and where it is likely to collect information about people who use that service – to be an aspect of that care. The regulations under the Public Services Reform (Scotland) Act 2010 must therefore be met when using surveillance in this way, particularly in respect of privacy and dignity.

Providers are also required to comply with the Data Protection Act 2018 and, since May 2018, the General Data Protection Regulation when processing personal data. Some providers will also have legal obligations under the Human Rights Act 1998, the Investigatory Powers Act 2016, the Regulation of Investigatory Powers Act 2000 and the Regulation of Investigatory Powers (Scotland) Act 2000. The Care Inspectorate does not provide direct scrutiny in respect of this legislation but we do expect providers to take account of relevant legislation and guidance. Providers may wish to seek legal advice about how to comply with their various legal obligations.

In addition to the above, the Mental Welfare Commission has published two best practice guides.

- Rights, Risks and Limits to Freedom (2013)
  http://www.mwcscot.org.uk/media/125247/rights_risks_2013_edition_web_version.pdf

Section 3.6 covers video surveillance in a care setting.

- Decision about Technology (2015)
  http://www.mwcscot.org.uk/media/241012/decisions_about_technology.pdf

This guidance outlines good practice when considering the use of telecare and assistive technology for people with dementia, learning disability and related disorders.

In addition to the legal requirements set out above, the Care Inspectorate expects people providing care to use Scotland's Health and Social Care Standards to plan and assess the quality of their care.

These standards, written from the perspective of the person experiencing care, state:

2.7 "My rights are protected by ensuring that any surveillance or monitoring device that I or the organisation use is necessary and proportionate, and I am involved in deciding how it is used".

They also set out the expectations about how people who lack capacity or have reduced capacity should be included in decisions about their care and support.

3. Understanding and defining the purpose for using surveillance systems

In any situation, data protection legislation requires that surveillance must only be used in the pursuit of one or more legitimate (reasonable, lawful and appropriate) purposes, and must be necessary, transparent, proportionate and fair, to meet an identified need. You must be able to identify a specific and explicit purpose(s) for your use of surveillance – what you want to achieve by using it.

If you determine that you have a valid purpose, you should consider whether surveillance is possibly the only way to achieve it. Could something else be done that would not involve the same intrusion into people's privacy?

You should also consider at this stage and keep under review whether your planned use of surveillance for the identified purpose(s) is likely to comply with the legally permitted' conditions for processing personal data.

Surveillance that is likely to gather sensitive or special categories of personal data will require you to meet additional conditions under the Data Protection Act 2018 and the General Data Protection Regulation. You can consider guidance produced by the Information Commissioner's Office (ICO) and may wish to seek legal advice if in any doubt.

You will need to consider in more detail whether the surveillance is necessary before you make any final decision, but you should consider at an early stage and keep under review whether alternative measures can meet the purpose you have identified.
You may wish to use surveillance for more than one purpose. If so, each of these purposes must be identified as necessary and proportionate in its own right.

Information gathered using surveillance for one purpose must not be used for another, incompatible purpose. For example, recordings made for the sole purpose of protecting vulnerable people from abuse should not be used as a record of staff time-keeping for disciplinary purposes.

You will also have to consider whether a Data Protection Impact Assessment (sometimes known as a Privacy Impact Assessment) should be carried out. This is a tool to help identify the most effective

way to comply with your obligations and reduce the risks of harm to individuals through the misuse of their personal information. You should check for relevant guidance published by the Information Commissioner's Office and may wish to consider seeking legal advice to ensure you are complying with your obligations under the General Data Protection Regulation.

Example

A care home provider is concerned that there has been a series of thefts from a communal, living area of the home. Alternative ways to prevent thefts or identify the thief are not suitable, as many people in the home are living with dementia or experience difficulties in communication. The provider therefore decides, after consultation with staff, residents, and their families that the prevention and detection of crime is a legitimate purpose to consider installing a surveillance system in the room for a limited period of time.

Record your purpose(s) and initial assessment of why surveillance is necessary to meet it. You should also document what alternatives to using surveillance you have considered and why they are not suitable, as this will be evidence to support any decision to use surveillance.

4. Needs assessment

The purpose you identify when proposing any surveillance must support the needs and interests of people using services.

This is particularly relevant where an identified purpose is to protect people from risks of unsafe care or treatment. You must decide whether their needs are met by surveillance and whether the intrusion is justified.

There may be competing and conflicting needs for people using your care service. Many of these tensions are inherent in the Health and Social Care Standards. For example, the Standards state that people can expect to live in an environment where they are free from abuse, harm and neglect (3.20), but they also state that people can expect to live in a homely environment (5.6). Use of surveillance may help the first of these, but impede the second. In considering whether to use surveillance, you will need to assess how it supports, or may limit, the needs and rights of all the people using your care service.

Example: Early Learning and Childcare

Many nurseries install CCTV with the primary purpose of monitoring people entering and leaving the building. This includes staff, parents and children. This helps to ensure that children are safe in the premises and that no unknown adults enter the building. We would expect the nursery to have a clear policy to let parents and staff know that it is installed and how it will be used.

5. Thinking about the information you will gather and in what circumstances

It is important to think about what information surveillance is likely to gather, including information gathered incidentally or inadvertently.

The more personal or sensitive the information that the surveillance is likely to collect, the greater the impact on people's privacy. A key issue for you to consider at this point is whether you plan to use covert or overt surveillance. As one of the data protection principles under the General Data Protection Regulation is transparency, there will be a presumption in favour of the use of overt surveillance and so you should consider this carefully.

People may behave differently if they know they are being observed, and this could help meet a purpose, such as the prevention of crime. It also means that covert surveillance has a greater impact on people's privacy as they are not able to change their behaviour as they would if they knew they were being observed.

You should also consider the potential of surveillance having a negative impact on the way staff interact with those they care for (if they know they are being monitored by overt surveillance). For example, staff may begin to deliver care in a process-driven way, rather than in a compassionate, person-led way.

Covert surveillance is more likely to capture sensitive, intimate or deeply personal information. This means that any decision to use covert surveillance must satisfy a more pressing purpose and legitimate aim than the use of overt surveillance to remain proportionate and lawful.

To remain lawful we would expect any covert surveillance to be limited in time and purpose. It should be used to deal with an identified problem, not put into regular, ongoing use.

As mentioned previously, for care providers that are public bodies, the use of covert surveillance will be subject to authorisation under, and compliance with, the Investigatory Powers Act 2016, the Regulation of Investigatory Powers Act 2000 and the Regulation of Investigatory Powers (Scotland) Act 2000.

6. Consultation

Using surveillance systems in a care setting is potentially intrusive to the privacy of people who use services, their families and friends, staff and other people who visit the service.

Consulting these people is the best way to understand their privacy concerns and ensure their views are taken into consideration. You should consult on the use of surveillance wherever it is possible to do so. The Health and Social Care Standards will help you think about the importance of involving people. The principles underpinning the Standards state "I am included in wider decisions about the way the service is provided, and my suggestions, feedback and concerns are considered".

The Standards state:

2.11. My views will always be sought and my choices respected, including when I have reduced capacity to fully make my own decisions.

2.12. If I am unable to make my own decisions at any time, the views of those who know my wishes, such as my carer, independent advocate, formal or informal representative are sought and taken into account.

Consultation is not a one-off exercise, but is something you should repeat throughout the process of considering and using surveillance. For example, it would be useful to consult:

- at an early stage, to establish the appetite for, or any significant concerns about, the use of surveillance
- when you have developed detailed proposals (when people can best understand what is being proposed)
- from time to time throughout the use of surveillance so that its impact can be kept under review
- when new people who will be affected by the surveillance start to use the care and support service you provide.

If you are currently using surveillance systems, you should consider consulting on their continued use.

The information you give to people you consult should cover:

- the type of surveillance you are considering
- where it would be used
- the purpose of it
- what information will be collected
- where and how it will be stored
- who will have access to the information and how long it will be kept for
- how it will be destroyed

Your consultation methods should be appropriate for the type of care and support service you provide, who will be affected, and the size of your service(s). You record in detail the process you followed and responses you received, and use this information to plan your approach.

You must give due consideration to the privacy concerns that are identified during consultation. In some limited circumstances, consultation will not be possible. For example, using surveillance in a targeted and time-limited way to investigate specific concerns of abuse may be prejudiced if possible perpetrators are tipped off by a consultation process. Where you decide not to consult on the use of surveillance, you will be expected to be able to explain and justify that decision.

Our inspectors may wish to see what steps you have taken to consult on the use of surveillance.

7. Consent for surveillance

As previously explained, any surveillance must meet relevant conditions for processing personal data (and, in some cases, sensitive personal data) under the Data Protection Act 2018 and obligations under the General Data Protection Regulation.

Explicit consent is just one example of a condition set out in legislation which provides a lawful basis for surveillance. However, it is not usually well suited to surveillance, since it is not normally possible to get valid consent of all visitors and people using the service.

For this reason, conditions that do not require consent of the individuals are usually relied on for most surveillance.

However, any surveillance that is used in a non-public place which captures sensitive or special category personal data about an individual (as legally defined, such as information about their health, sexual life, race or religion) is likely to require the explicit consent of that individual to be lawful. This is also the case when gathering information that is particularly intrusive of a person's privacy (even where it is not the specific intention to do so).

For example, a camera in the private room of a person who experiences care is likely to require the consent of that person, but other lawful conditions under the Data Protection Act 2018 may be available so that consent is not required from other people who may enter the room. It is unlikely to be lawful to use surveillance to directly observe a person's medical treatment, intimate care, or someone practicing their religion in a private place (such as a dedicated prayer room) without the explicit consent of that person, even if the purpose of the system is to observe something else.

If you are considering surveillance of this type and you cannot obtain or do not intend to seek explicit consent, we suggest you first obtain specialist legal advice.

Explicit consent should be absolutely clear. The person must be informed and understand:

- how their information will be gathered
- what type of information will be gathered (or even the specific information)
- the purposes of gathering the information
- how the information will be used, accessed, secured and ultimately destroyed
- any special aspects that may affect the person, such as any disclosures that may be made.

Where consent is required, it must be freely given (it cannot be obtained by coercion or threat) and a provider cannot infer consent from a non-response to a request for consent. When using consent as a basis for surveillance, the person must have a right to withdraw that consent.

It is important that any refusal, or withdrawal, of consent – where consent has been asked for – is respected.

The initial consultation process should not be seen as an exercise in seeking consent.

Example

A person who experiences care in their own home feels vulnerable and concerned about having carers in her house and raised this concern with the provider of her care. A CCTV system in her home, which can be switched on during visits from carers or at other times when she feels vulnerable, is considered as an option. The consent of the person would be required to make this lawful. Care staff attending the person's home should be notified about the cameras, and consideration given as to whether their explicit consent is required.

Example

A CCTV system in a prayer room is likely to capture images of people privately observing their religion, which is sensitive personal data (a special category of personal data under the General Data Protection Regulation). It is likely that explicit consent of people using the room for prayer would be required, unless the purpose of the system is in the substantial public interest by preventing or detecting any unlawful act, and obtaining explicit consent would prejudice that aim.

You must establish that you have a lawful basis for your proposed use of surveillance.

If consent is used as a basis for surveillance, you must keep appropriate records. Consent must be fairly and lawfully obtained, and refusal of consent must be respected.

Our inspectors may wish to see these records to help them understand how you have come to your decisions.

8. Capacity to consent and to contribute to a consultation

As a care service provider, you will be familiar with the statutory principles of the Adults with Incapacity (Scotland) Act 2000. This Act provides the legal requirements to support and enable individuals who lack capacity.

If someone lacks capacity it is unlikely that you will be able to rely on consent to use surveillance. You will not be able to seek that consent from others, such as their family, unless the other person has relevant powers under a health and welfare lasting power of attorney or a guardianship order.

Where explicit consent is likely to be required to use surveillance lawfully, for example in the room of an individual, and it is established that the individual lacks mental capacity, it would not be appropriate for you to make a decision or attempt to provide explicit consent on behalf of the individual, in the absence of a relevant power of attorney, even when acting in accordance with the Adults with Incapacity (Scotland) Act 2000. A decision made in accordance with the Act does not have the same legal status as consent and should not be relied on as justification for using surveillance.

In some situations, a family member, friend or other individual may be a welfare power of attorney or welfare guardian for the person who lacks capacity. It is unlikely that they would have been granted specific decision making powers to initiate or consent to surveillance, but they may have some general powers to take or be consulted about decisions relevant to their care. That may extend to considering surveillance depending on the purpose for it. A welfare guardian could also make an application to a sheriff to have a specific power granted. If someone has a welfare power of attorney or guardianship for a person who lacks capacity you may be able to consult and seek consent from them. However, if you are in any doubt about whether they can consent to surveillance you should consider seeking legal advice.

Whenever you are consulting on, or considering, the use of surveillance, you must also carefully consider and apply the principles under the Adults with Incapacity (Scotland) Act 2000 in relation to any individuals lacking in mental capacity. You should consider whether and how you can support and enable them to express their views about privacy, take account of the wishes of the person and consult with their primary carer, nearest relative, named person, attorney or guardian as appropriate. You should also consider whether the use of surveillance would benefit the individual and whether it is the least restrictive option available to address the identified need.

A lack of mental capacity must not be used as an excuse to ignore or dismiss the right of privacy of any person. The Health and Social Care Standards state:

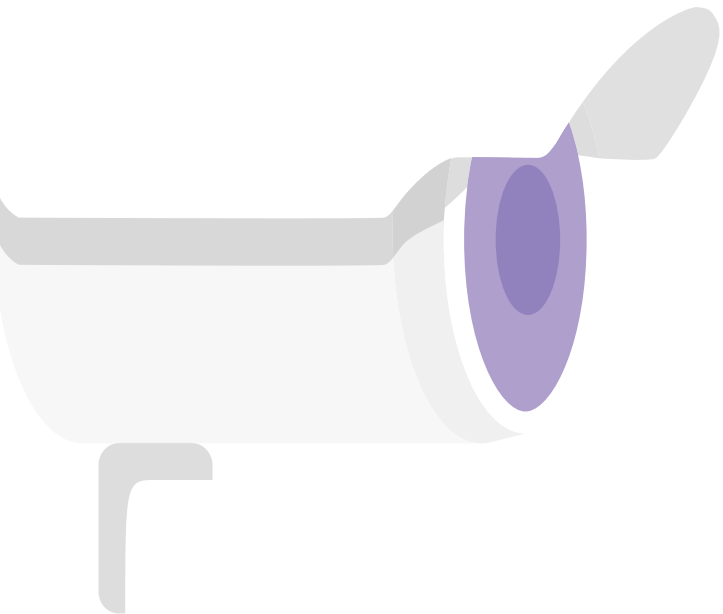
2.11. My views will always be sought and my choices respected, including when I have reduced capacity to fully make my own decisions.

2.12. If I am unable to make my own decisions at any time, the views of those who know my wishes, such as my carer, independent advocate, formal or informal representative are sought and taken into account.

You should therefore take special care to record how you have handled the interests of people who lack mental capacity when consulting on the use of surveillance and in particular, any consent-based, or more privacy intrusive use.

You will need to regularly review whether people deemed to lack capacity continue to lack capacity. Therefore, those previously deemed without mental capacity when decisions were made about the use of surveillance should be informed and consulted with, and their consent obtained as appropriate when they are deemed to have capacity.

If you have concerns that a person who lacks capacity to consent, or any other vulnerable person, may be being abused, you should report this through local adult support and protection processes or, if there is an immediate risk, to Police Scotland.



9. Protecting privacy and treating people with dignity and respect

You should take steps to address any concerns about surveillance that have been raised by people experiencing care or their families, with the aim of minimising the potential impact on privacy. It is not up to others to identify all the relevant concerns – as the care provider it is your responsibility to be aware of the need to treat people with dignity and respect.

Some privacy protections will be relevant to all surveillance, such as ensuring that only authorised people can access the information collected. Other protective measures may depend on the particular situation and the privacy risks that have been identified.

This could include taking steps such as:

- repositioning cameras or audio recording equipment, or limiting the times they are used, to capture less sensitive information, information about fewer individuals, or to avoid capturing behaviours that may be more intrusive on people's privacy (such as intimate care)
- seeking to gather information that is less identifiable, for example statistical information from sensors instead of video
- allowing staff or people experiencing care to turn off a surveillance system at certain times
- following the Information Commissioner's Office CCTV Code of Practice and the Surveillance Camera Code of Practice on the positioning and use of CCTV cameras.

You should avoid wherever possible recording sensitive information, such as intimate or personal care or people privately observing their religious beliefs. You should minimise using surveillance that potentially intrudes on people's privacy, such as indiscriminate recording of audio in semi-public or private places.

Cameras worn by care staff providing intimate or personal care will be particularly intrusive. If these cameras are used, they should be switched off while intimate care is being delivered.

As detailed above, types of surveillance that intrude on privacy will require a greater justification and need to meet higher requirements to remain lawful.

Documenting how you have addressed privacy concerns, or where you are unable to and why, will be invaluable in helping to make your final decision. Our inspectors may wish to view the steps you have taken to understand why you have made your decisions.

You must balance your legitimate and necessary aim against the privacy concerns and intrusion of those affected to decide if the surveillance is fair and proportionate. These decisions should be made by an appropriate and senior person or group within your provider organisation, and clear records of their consideration, decision and reasons must be retained.

If you are a public body, subject to the requirements of the Regulation of Investigatory Powers legislation, the decision to use covert surveillance may only be made by an authorising officer who is empowered to do so under the Act.

Any use of covert surveillance under Regulation of Investigatory Powers legislation must be undertaken in line with your established policies.

Example

Some residential children's services use CCTV to monitor all communal areas because children and young people have told staff it makes them feel safe and can help prevent bullying. It may be justifiable to use CCTV, depending on the circumstances and the outcome of consultation and any Data Protection Impact Assessment carried out.

10. Additional consideration relating to deprivation of liberty and restraint

Restraint takes place when the planned or unplanned, deliberate or unintentional actions of care staff prevent a person from doing what he or she wishes to do and as a result places limits on his or her freedom of movement.

It should be used only where there is absolutely no alternative that would reduce an identified, specific risk to the person concerned to an acceptable level. It should be a 'last resort' intervention. If using restraint in a care setting, this needs to be done in a way that respects human rights and complies with the law and relevant care regulations.

In some circumstances, surveillance systems could be used for purposes that might fall within the definition of 'restraint'. For example, the use of CCTV or radio-frequency identification (RFID) tracking devices to monitor someone's location or to assist people with impaired capacity, to function as independently as is practicable.

If the identified purpose or use of surveillance has the potential to act as a restriction or deprivation of liberty, you must take special care to consult and to consider the relevant guidance. This is in addition to the usual considerations you must make on the use of surveillance.

You should be aware that restraint as defined in the Mental Welfare Commission for Scotland's "Rights, Risks and Limits to Freedom" includes the restriction of movement of a person lacking capacity, whether the person is resisting or not.

You should also take account of the Health and Social Care Standards which state that:

1.3. If my independence, control and choice are restricted, this complies with relevant legislation and any restrictions are justified, kept to a minimum, and carried out sensitively.

The law relating to restraint is complex and you may wish to consider seeking legal advice.

11. Safety, suitability and maintenance of equipment

Any surveillance system must be suitable for its intended purpose. For example, a CCTV system that needs to be able to visually identify a person will not meet its purpose if the resolution of the images is not high enough or the lighting is too dim.

Meta-data, such as the date, time and location of a recording, should be collected and retained as appropriate to support the purpose.

The equipment should be maintained regularly to ensure it is working correctly and remains suitable for its purpose.

In particular, you must assess whether any surveillance equipment may represent a risk to health and safety and take appropriate steps to mitigate it.

Example

We know of some instances where people with severe epilepsy may have a camera in their room for monitoring purposes. If, for example they have a seizure overnight staff can respond quickly to ensure the person is safe and attended to.

12. Staff training and record keeping

Controls must exist to ensure that only appropriate and authorised people are given access to any information recorded, for example by placing monitors for viewing CCTV images in a lockable office, where only an appropriate manager can access them.

Only people with a legitimate and lawful need to access private information obtained by surveillance should have access to that information.

You must ensure that adequate security is in place to prevent unauthorised access – the more sensitive and private the information, the greater the required level of security. You must also implement appropriate technical and organisational measures to protect the security of any data collected through surveillance

Information being stored or transmitted electronically must be kept secure through the use of strong passwords and appropriately secure software and encrypted if appropriate.

If information is being stored on your behalf by a third party (for example, on a web-based server) you are still responsible for ensuring that it is kept secure.

Staff who are authorised to have access to information gathered by surveillance should have appropriate training on its use.

You should keep a record of when and why recorded information has been accessed.

When you record information with surveillance, you have statutory obligations under the Data Protection Act, General Data Protection Regulation and, in the case of public authorities, the Freedom of Information (Scotland) Act 2002, which may create a right of access to the information.

You should have clear policies and procedures in place for handling requests for access to recorded information, on sharing and disclosing information, and on handling complaints about the use of surveillance (for example, where someone considers that the use of surveillance is causing harm or distress).

You should also have clear policy on the secure retention and destruction of information in accordance with relevant legislation and guidance.

13. Informing people

Wherever possible, you should ensure that staff, people experiencing care and support and all visitors are informed about the use of surveillance. Consider whether they can be notified in general terms about the use of covert surveillance, if this does not prejudice the purpose.

Part of this may be achieved with an appropriate privacy notice and physical signage, but this alone is unlikely to be enough and you should undertake it in a way that is consistent with maintaining a homely environment. You should consider the capacity of those likely to be affected and decide the most appropriate way to communicate, following the principles of the Adults with Incapacity (Scotland) Act 2000. You should also consider people's differing physical needs as this may affect how you inform and communicate with them.

The Health and Social Care Standards state:

2.9. I receive and understand information and advice in a format or language that is right for me.

2.10. I can access translation services and communication tools where necessary and I am supported to use these.

If you use surveillance, you are required to register as a data controller with the Information Commissioner's Office. Many providers will already be required to be registered anyway, but you should ensure that your registration is adequate to cover the use of surveillance.

14. Operating the surveillance system

You should have a clear policy and a record of who in your organisation is responsible for the operation and maintenance of any surveillance system, and the protection, management and control of the information obtained using surveillance.

15. Surveillance equipment installed by people who use the service, or their relatives

From time to time, people naturally worry about whether a loved one is being properly cared for. Where they are being looked after in a health or social care setting, there will be times when relatives and friends may be concerned because they cannot see directly what is going on. They may think about using a hidden camera or audio recording device to reassure themselves about the care their loved one is receiving.

If you discover that someone is using covert or overt surveillance in your service, the welfare and care of the person using the service must remain your primary consideration. Even if the use of the camera breaches a contract of service, the continuity and safety of the person's care must be ensured.

If someone has decided to use surveillance in your service, it may well arise from a significant fear or concern about the quality of care or the welfare of a vulnerable person. It may indicate a problem that you were not aware of, and it is very important that you investigate and understand. In some cases, this may even lead you to think about undertaking your own surveillance, with consideration of the information in this document.

The person using the service or their friend or relative should not suffer any detriment of care or consideration if you discover that they have used surveillance without your knowledge. As with any other circumstance where concerns are raised, we would expect you to follow appropriate procedures to investigate and respond.

If you are concerned that the surveillance may be unreasonably intruding on the privacy or rights of a person experiencing care or others, then you will want to ensure this is properly assessed and make a decision about the continued use of the surveillance equipment, including the position relating to consent and safeguarding circumstances.

Deliberately damaging a surveillance device, deleting recordings or removing the device with the intention of not returning it to its legal owner is likely to be a criminal offence. However, switching a camera off or removing it for safe return to its owner would be unlikely to be an offence. In any case, you should consider seeking legal advice.

16. The Care Inspectorate and the use of information recorded using surveillance

The Care Inspectorate's powers allow us to have access to information that has been recorded using covert or overt surveillance (or to have access to surveillance systems) where we consider it necessary and proportionate to do so to exercise our functions as a scrutiny and improvement body.

However, we would not routinely access this information. We may ask to access these recordings where we believe they may help us understand the quality and safety of the care provided, or in assessing your compliance with the standards of care set out in regulations.

Where we receive or access a recording that shows abuse, or poor or unsafe care, we will, of course, act on that information where we can do so lawfully.

References

Adults with Incapacity (Scotland) Act 2000

Data Protection Act 2018

Public Services Reform (Scotland) Act 2010

Human Rights Act 1998

Investigatory Powers Act 2016

Regulation of Investigatory Powers Act 2000

Regulation of Investigatory Powers (Scotland) Act 2000

Rights, Risks and Limits to Freedom, Mental Welfare Commission (MWC, 2013)

Decisions about technology, Mental Welfare Commission (MWC, 2015)

The Information Commissioner's Office guide to data protection – A general guide to complying with the Data Protection Act.

The Information Commissioner's Office Code of Practice on CCTV – Complying with the Data Protection Act in relation to CCTV

In the picture: A data protection code of practice for surveillance cameras and personal information, Information Commissionerhttps://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

The Information Commissioner's Office: Data Protection. The employment practices code https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

The Information Commissioners Office: Conducting Privacy Impact Assessments. Code of Practice https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

References to Legislation

The links to legislation are links to the government's website – www.legislation.gov.uk. It is understood that the primary legislation (Acts of Parliament and Acts of The Scottish Parliament) displayed on that website is displayed in its up-to-date form, i.e. amendments made to an Act since it was originally enacted are incorporated on the version displayed.

The Care Inspectorate does not offer any assurances that any of the legislation on this website is accurately reproduced. Any person relying on it does so at their own risk and the Care Inspectorate will not be responsible for any loss or damage suffered by any party as a result of their reliance on the terms of the legislation referred to.

Headquarters
Care Inspectorate
Compass House
11 Riverside Drive
Dundee
DD1 4NY
Tel: 01382 207100
Fax: 01382 207289

Website: www.careinspectorate.com
Email: enquiries@careinspectorate.com
Care Inspectorate Enquiries: 0345 600 9527

This publication is available in alternative formats on request.

© Care Inspectorate 2018 | Published by: Communications | COMMS-0618-238

@careinspect careinspectorate

Illustration for front cover designed by Kjpargeter/Freepik
Illustrations inside document designed by Macrovector/Freepik

We are a Living Wage Employer
Investing in Volunteers
Healthy Working Lives Gold Award
Investors in Young People Good Practice Award
Carer Positive Employer in Scotland Engaged
Corporate member of Plain English Campaign 420 Committed to clearer communication