

CCTV Policy

CM08

Date Written	
Author(s)	
Version	
Date Signed Off	
Reviewed by	

Date: []

Review Data

Initial Production

Name	Role/Department	RACI	Date

R = Responsible for writing the policy; **A** = Accountable; **C** = Consulted; **I** = Informed

Change History

Version	Date	Details of Change	Author

Emergency Contact Details

Name	Email	Mobile

CQC Fundamental Standards

Regulation Number	Regulation Details
Regulation 17: Good governance	Providers must have effective governance, including assurance and auditing systems or processes which must assess, monitor and mitigate any risks relating the health, safety and welfare of people using services and others.

Key Lines of Enquiry

KLOE	How this applies to CCTV
Safe	The lawful use of CCTV can contribute to ensuring safe, effective, compassionate and high-quality care.

Related Documents

This policy should be read in conjunction with our:

- HR05 - Disciplinary and Grievance Procedures Policy



Policy Aims

To ensure that any use of surveillance is lawful, fair and proportionate – and used for purposes that support the delivery of safe, effective, compassionate and high-quality care.



Key Question: Why is CCTV used?

The most common uses of surveillance systems, such as CCTV, are a way to enhance the security and safety of premises and property, and to protect the safety of people. Surveillance may also be used as a tool to help protect people from the risk of abuse, or to investigate allegations or serious concerns about possible abuse or crime.

Surveillance systems may also be an effective way to promote and support the independence and autonomy of people who use care services, by monitoring their welfare with the use of 'Telecare' systems, while minimising the restriction on their movements and activities.

In some circumstances, and with the required safeguards, surveillance systems may be used as part of the appropriate deprivation of someone's liberty – for example, to monitor and identify if a person living with dementia is leaving a care home.

Careville Ltd acknowledges that there are significant benefits to using surveillance. However, we are mindful of the potential repercussions, and therefore use it in conjunction with other, less intrusive methods such as:

- Always having enough capable and confident staff on duty with the right mix of skills.
- Encouraging an open culture, where both staff and people who use services are able to raise any concerns, and ensuring that those concerns are addressed.
- Ensuring supervision and appraisal are used to develop and motivate staff and, where required, review their practice or behaviour.

Definitions

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

Overt surveillance is where the individual being monitored would reasonably be aware of the surveillance occurring. For example, visible CCTV cameras with clear signs saying that they are in use.

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

Surveillance systems are the technology and equipment used to carry out surveillance, or to store and process the information gathered. Advances in technology mean that new systems or methods may become more commonplace. For simplicity in this information we will generally refer to 'surveillance', which could encompass CCTV, Wi-Fi cameras, audio recording, radio-frequency identification (RFID) tracking and many other types of system. This information sets out considerations that can be applied to these and any other existing or emerging technologies.

Privacy in its broadest sense, is the right of an individual to be left alone. Intrusion into privacy can include the collection of information through surveillance or monitoring of how people act in public or private space.

Needs Assessment

The purpose for the proposed use of any surveillance will be assessed on how it will support the needs and interests of people using services.

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

Protecting Privacy and Treating People with Dignity and Respect

Careville Ltd takes steps to address any concerns about surveillance that have been identified from people who use services or their families, with the aim of minimizing the potential impact on privacy. These steps include:

- Repositioning cameras or audio recording equipment, or limiting the times at which they are in use, 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 using the service, to turn off a surveillance system at certain times.
- Following the ICO's CCTV Code of Practice, and the Surveillance Camera Code of Practice, on the positioning and use of CCTV cameras.

Recording sensitive information, such as intimate care or people privately observing their religious beliefs, should be avoided wherever possible. More privacy intrusive surveillance, such as indiscriminate recording of audio in semi-public or private places should be minimised.



Key Question: Who needs to be consulted when using CCTV?

The use of surveillance systems in a care setting has the potential to be intrusive to the privacy of service users, their families and friends, staff, trade unions and other people who visit.

Consultation with these people is the best way to understand their privacy concerns. Providers should consult on the use of surveillance wherever it is possible to do so.

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

- At an early stage of consideration (to establish the appetite for, or any significant concerns about, the use of surveillance).
- When detailed proposals have been developed (when people can best understand what is being proposed).
- And from time to time throughout the use of surveillance (so that the impact of its use can be kept under review).

The information provided to people involved in the consultation should cover:

- The type of surveillance being considered.
- Where it is being considered for use
- The purpose of the proposed surveillance.
- 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.

Consent

Any use of surveillance must meet relevant conditions for processing personal data (and, in some cases, sensitive personal data) under the Data Protection Act 2018 (DPA).

Consent ('explicit' consent for sensitive personal data) is just one example of a DPA condition that 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 relied on for most surveillance.

However, any surveillance that is used in a non-public place for the purpose of capturing more sensitive personal data about an individual (such as information about their health, sexual life, race or religion) is likely to require 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.

Workplace Example

For example, a camera in the private room of a person who receives care is likely to require the consent of that person, but other lawful conditions under the DPA may be available so that consent is not required from other people who may enter the room (visitors, staff etc.)

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.

Explicit consent should be absolutely clear. The individual must be told:

- 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 and accessed
- any special aspects that may affect the individual, 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 to be seen as an exercise in seeking consent.

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 identify an individual person will not meet its purpose if the resolution of the images is not high enough or the lighting is not sufficient.

Staff Training and Record Keeping

- Only appropriate and authorised people are given access to any information recorded.
- Only people with a legitimate and lawful need to access private information obtained by surveillance have access to that information. Careville Ltd ensures that security is in place to prevent unauthorised access – the more sensitive and private the information, the greater the required level of security.
- Information being stored or transmitted electronically must be kept safe through the use of strong passwords and appropriately secure software.
- Staff who are authorised to have access to information gathered by surveillance have appropriate training on its use. A record is kept of when and why recorded information has been accessed.

When recording information via surveillance systems, there will be statutory obligations on care providers under the DPA and – for public authorities – the Freedom of Information Act 2000, which may create a right of access to the information.



Key Points to Take Away

- Careville Ltd acknowledges that there are significant benefits to using surveillance. However, we are mindful of the potential repercussions, and therefore use it in conjunction with other, less intrusive methods.
- The purpose for the proposed use of any surveillance will be assessed on how it will support the needs and interests of people using services.
- Any use of surveillance must meet relevant conditions for processing personal data (and, in some cases, sensitive personal data) under the Data Protection Act 2018 (DPA).
- 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.

Policy Review

A Director will review this policy at least once a year to make any updates needed.

Authorisation and Signature

This Policy is the authorised version agreed by the Directors of **Careville Ltd**. All employees are expected to follow this policy and failure to do so could result in disciplinary action.

Director's Signature

Director