OPSR14 CCTV POLICY

Policy area:	Operations (Residential)
Title of policy:	OPSR14 CCTV
Version:	V1 – September 2020
Effective date:	22 October 2020
Approved by:	Chief Operating Officer
Approved date(s):	22 October 2020
Revision date:	As required

Scope

Policy Statement

This organisation is aware of its responsibilities in the use of CCTV equipment and of the need to ensure it is fully compliant with relevant legislative requirements. This policy sets out the use and the safeguards in place of any type of CCTV or surveillance equipment on any premises owned or leased by the company. Within the Health and Social Care Sector, the case of surveillance equipment has risen markedly in the last 5 years. There have also been case law judgements, in particular relation to privacy issues, which has led to the new Code of Practice from the Information Commissioners' Office (ICO) issued in June 2015.

The Policy

The organisation do not have CCTV operating within any of the organisations premises.

If the organisation do choose to implement CCTV this policy will be updated to incorporate a full disclosure of our use, retention and security measures with regards to CCTV.

The care homes do currently have thermal imaging recognition cameras operating at the entrances as an infection control measure. These images are used with the sole purpose to assist in our endeavour to enhance infection control measures to protect our staff and residents from risk of infection. These images are stored in a secure location for a period of time in accordance with our data retention policy. These images will not be shared with any third party without the express permission of the data subject involved.

Principles

Careful consideration needs to be given as to the reasoning behind the introduction of any type of surveillance system.

The general public need to be aware of any covert usage.

Staff, where possible, should be included in discussions about the use of such systems.

Individual Residents or residents must be fully involved in decisions regarding the usage of such equipment. Where they lack capacity, as defined by the M.C.A. 2005, a best interest decision will be taken, following the guidance in the Act.

Code of Practice

The first Code was introduced in 2000 and since then the use of CCTV has moved to a much more sophisticated system of digital and increasingly portable technology. Privacy has become an issue in the use of such systems and the Code aims to keep users of such systems on the right side of the law. The Code provides good practice advice for those involved in operating CCTV and other surveillance camera devices that view or record individuals e.g. vehicle registration using ANPR (automatic number plate recognition).

The Protection of Freedoms Act (POFA) has introduced a new Commissioner, the Surveillance Camera Commissioner to promote the Code. It is designed to help those who use surveillance cameras to collect personal data to stay within the law.

The terms 'surveillance system(s)', 'CCTV' and 'information' are used throughout the Code for ease of reference. Information held by organisations that is about individuals is covered by Data Protection Legislation and the guidance in the Code will assist organisations to comply with these obligations.

This Code of Practice is consistent with the POFA Code and there is a Memorandum of Understanding between the Information Commissioner and Surveillance Camera Commissioner. The Code covers the use of surveillance systems which are used to monitor or record the activities of individuals, or both. As such, they process individuals' information – their personal data. Most uses of surveillance systems will therefore be covered by the DPA and the provisions of the Code, whether the system is used by a multi-national company to monitor entry of staff or visitors, or a local newsagent recording information to help prevent crime.

The Code also covers the use of camera related surveillance equipment including:

- Automatic Number Plate Recognition (ANPR)
- Body worn video (BWV)
- Unmanned aerial systems (UAS) and
- Other systems that capture information of identifiable individuals or information relating to individuals.

The Code provides guidance on information governance, such as data retention and disposal.

It is important that the Data Controller of the organisation is fully conversant with the Code of Practice and the principles set out below.

Appendix 1

Data Protection Legislation

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-
    - at least one of the conditions in Schedule 2 is met, and

  - in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

- Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- Personal data shall be accurate and, where necessary, kept up to date.

- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

- Personal data shall be processed in accordance with the rights of data subjects under this Act.

- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This is not a full explanation of the principles.
For more general information, see the following Legal Guidance:
The ICO's "Data Protection Act 1998 Legal Guidance" is available on the ICO website: www.ico.org.uk

Appendix 2

The Guiding Principles of the Surveillance Camera Code of Practice

System operators should adopt the following guiding principles:

- Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
- The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

- There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
- There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
- Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
- No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
- Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
- Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
- Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
- There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
- When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
- Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.
- In communal areas we consult with those where the fitting of such cameras may impact their privacy.
- In bedroom areas consent as defined by the Mental Capacity Act 2005 is sought as this setting would be covered by the handling of sensitive personal data under the Data Protection Act 2018
- We are aware of the Care Quality Commission guidance of the use of CCTV in a social care setting and we have adopted the checklist contained in the Code of Practice which will be reviewed annually.

Definitions

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

Overt surveillance. Where the individual being monitored would reasonably be aware of the surveillance occurring, e.g. visible CCTV cameras with clear signage that they are in use.

Covert surveillance. Where the individual being monitored would not be reasonably aware of the surveillance occurring e.g. the use of hidden audio recording devices for a time-limited and specific purpose.

Surveillance systems. The technology or equipment used to store or process the information gathered and advances in technology means it encompasses CCTV, Wi-Fi cameras, audio recording, radio frequency identification (RFID), smartphone apps etc.

This policy excludes the use of medical devices or treatment that gathers information, any use of technology with the knowledge and explicit consent of the patient e.g. filming a surgical procedure, or any communication system controlled by the person using it, e.g. webcams, alarm buttons etc. These would not be considered as surveillance but issues of privacy still need to be considered.

Contact point for future privacy concerns: email: dpo@careportgroup.com

Related Policies

Adult Safeguarding

Confidentiality

Consent

Cyber Security

Data retention policy

Data Protection Legislative Framework (GDPR)

Related Guidance

- ICO CCTV https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/scenarios/cctv/
- Gov.UK Surveillance camera code of practice https://www.gov.uk/government/publications/surveillance-camera-code-of-practice
- CQC Using surveillance: information for service providers https://www.cqc.org.uk/guidance-providers/all-services/using-surveillance-information-service-providers

Training Statement

All staff responsible for data control receive training in relation to CCTV.

All staff, during induction are made aware of the organisations policies and procedures, all of which are used for training updates. All policies and procedures are reviewed and amended where necessary and staff are made aware of any changes. Observations are undertaken to check skills and competencies. Various methods of training are used including one to one, on-line, group meetings, individual supervisions and external courses are sourced as required.