


# CCTV CODE OF CONDUCT

*(this organisation does not currently use CCTV, however this Code of Conduct is relevant to staff, visitors and residents' so called 'smart phones', baby monitors and Data Protection)*

|                        |                          |  |
|------------------------|--------------------------|--|
| <b>VERSION No</b>      | <b>3</b>                 |  |
| <b>REVIEWED BY</b>     | <b>Mariana Philipova</b> |  |
| <b>NUMBER OF PAGES</b> | <b>6</b>                 |  |

## 1. 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.

- ! **ALL STAFF WORKING AT THIS HOME (WHILST ON SHIFT, ATTENDING TRAINING, STAFF MEETING OR JUST VISITING) MUST PLACE AND LOCK THEIR SMART PHONE IN THEIR LOCKERS AT ALL TIMES.**
- ! **ALL STAFF MUST NOT TAKE ANY VIDEO RECORDINGS OF EVEN PHOTOGRAPHS OF THE HOME INCLUDING PREMISES, GARDEN, OTHER STAFF, RESIDENTS, VISITORS, ETC!!**

## 2. 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 service users 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.**

## 3. Code of Practice

- a) 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).
- b) 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.
- c) 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 the Data Protection Legislation and the guidance in the Code will assist organisations to comply with these obligations.
- d) 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 which is 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.

- e) The Code also covers the use of camera related surveillance equipment including:
- ✚ Automatic Number Plate Recognition (ANPR)
  - ✚ Body worn video (BWV), such as ‘smart phone’
  - ✚ Unmanned aerial systems (UAS) and
  - ✚ Other systems that capture information of identifiable individuals or information relating to individuals.
- f) The Code provides guidance on information governance, such as data retention and disposal. It is important that the Data Controller of the organisation, the administrative assistant, is fully conversant with the Code of Practice and the principles set out below.

## *Appendix 1*

### **THE DATA PROTECTION LEGISLATION: DATA PROTECTION PRINCIPLES**

1. *Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-*
  - (a) *at least one of the conditions in Schedule 2 is met, and*
  - (b) *in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.*
2. *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.*
3. *Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.*
4. *Personal data shall be accurate and, where necessary, kept up to date.*
5. *Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.*
6. *Personal data shall be processed in accordance with the rights of data subjects under this Act.*
7. *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.*
8. *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<sup>1</sup>. The ICO’s “Data Protection Legislation Legal Guidance” is available on the ICO website: [www.ico.org.uk](http://www.ico.org.uk)*

## THE GUIDING PRINCIPLES OF THE SURVEILLANCE CAMERA CODE OF PRACTICE

*Staff operating surveillance camera system should adopt the following 12 guiding principles:*

- 1. 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.*
- 2. 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.*
- 3. 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.*
- 4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.*
- 5. 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.*
- 6. 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.*
- 7. 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.*
- 8. 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.*
- 9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.*
- 10. 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.*
- 11. 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.*
- 12. 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.*





*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.*
- Cover 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, baby monitors 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.*

## 4. Privacy

- a) *Privacy, in its broadest sense, is the right of the 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 spaces.*
- b) *It is therefore important that all factors are taken into consideration and clearly recorded, before the decision to undertake any form of surveillance is authorised.*
- c) *A **Privacy Impact Assessment (PIA)**, where appropriate, must be completed, following the guidance issued by the ICO. Using the following screening questions will assist in determining whether a PIA is necessary.*
- d) *'Yes' as the answer to any of the questions will indicate that a PIA would be a useful exercise:*
- i. *Will the surveillance involve the collection of new information about individuals?*
  - ii. *Will the surveillance compel individuals to provide information about themselves?*
  - iii. *Would such information be disclosed to organisations or people who previously had routine access to it?*
  - iv. *Would such information be used in a way it is not currently used for, or in a way it is not currently used?*
  - v. *Will the surveillance result in us making decisions or taking action against the individuals in ways which can have a significant impact on them?*
  - vi. *Would the surveillance require you to contact individuals in ways which they may find intrusive?*
- e) **If a PIA is deemed necessary, then complete the 6 steps below:**
- i. **Step One: Identify the need for a PIA:**
    -  *explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties*
    -  *linking to other relevant documents related to the project, for example a project proposal will be helpful*
    -  *summarise why the need for a PIA was identified (this can draw on your answers to the screening questions)*
  - ii. **Step Two: Describe the information flows:**
    -  *The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data*

flows. You should also say how many individuals are likely to be affected by the project.

 **Consultation requirements**

- Explain what practical steps you will take to ensure that you identify and address privacy risks
- Who should be consulted, internally and externally?
- How will you carry out the consultation? You should link this to the relevant stages of your project management process
- Consultation can be used at any stage of the PIA process.

iii. **Step Three: Identify the privacy and related risks**

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register. Annex three can be used to help identify the DPA related compliance risks.

| Privacy issue | Risk to individuals | Compliance risk | Associated organisation / corporate risk |
|---------------|---------------------|-----------------|--|
|               |                     |                 |  |

iv. **Step Four: Identify privacy solutions**

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

| Risk | Solution(s) | Result: the risk eliminated, reduced, or accepted? | Evaluation: the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project? |
|------|-------------|--|--|
|      |             |  |  |

v. **Step Five: Sign off and record the PIA outcomes**

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

| Risk | Approved solution | Approved by |
|------|-------------------|-------------|
|      |                   |             |

vi. **Step Six: Integrate the PIA outcomes back into the project plan**



Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork?



Who is responsible for implementing the solutions that have been approved?



*Who is the contact for any privacy concerns which may arise in the future?*

| Action to be taken | Date for completion of actions | Responsibility for action |
|--------------------|--------------------------------|---------------------------|
|                    |                                |                           |

**5. Training Statement**

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

**Related Policies**

*Adult Safeguarding*

*Confidentiality*

*Consent*

*Cyber Security*

*Data Protection*