Info centre

Guide

CCTV monitoring

CCTV in the UK

Increasingly, CCTV has become the principal method of carrying out surveillance of areas that may be accessed by the public as well as becoming commonplace in many workplaces in a variety of industries.

CCTV has an obvious crime-prevention and public safety role in the high street and in places such as shops and car parks. While this involves intrusion into the lives of ordinary people as they go about their day-to-day business, this is a generally accepted trade-off against the benefits CCTV offers.

However, the use of CCTV in the workplace as a means of observing staff is both less obviously beneficial, and considerably less accepted. Employers who use CCTV in the workplace need to ensure that doing so does not undermine trust in the employer-employee relationship, as well as ensuring that its use complies with regulatory and statutory requirements. Employers are advised to bear in mind the ICO's CCTV guidance, which recognises the special considerations that apply in the workplace and assists employers in complying with their legal obligations.

Dummy and non-operational CCTV

Dummy CCTV systems can act as a deterrent to offer some of the security and safety benefits afforded by operational systems - at a fraction of the cost. The DPA applies only where images are captured by CCTV that

Key points

- Employers should note that most CCTV systems are covered by the Data Protection Act 1998 (the DPA). They should therefore familiarise themselves with the requirements of the DPA and the CCTV Code of Practice issued by the Information Commissioner's Office (the ICO).
- Before installing a CCTV system, an impact assessment should be carried out to assess whether the use of CCTV is justified or whether another, less intrusive solution (such as improved lighting in a car park), could achieve the same objectives.
- A policy regarding the use of CCTV systems by camera operators and retention of images should be implemented.
- Warning signs should usually be posted, and the organisation must ensure it is able to comply with data subject access requests for images.
- It is estimated that there are around 1.85 million CCTV cameras in use in the UK, one for every 34 people.
- The vast majority of these cameras are operated by private companies on private premises, for example in workplaces.
- CCTV technology now goes further than simply recording people's movements to incorporate number plate and facial recognition, and, in some cases, adding listening functionality.

Legislation

contains 'personal data'. If no image is captured, by definition no personal data is processed, so the DPA does not apply, and there can be no infringement of privacy. Therefore, the guidance in this chapter does not apply to the use of dummy or non-operational CCTV systems.

Data Protection Act 1998

The DPA is the major legal control over CCTV surveillance in the UK, both within and outside the workplace. Most images recorded by CCTV systems will constitute 'personal data' for the purposes of the DPA, for example, where someone is identifiable from the images captured, or where other information relating to a living individual is caught, such as a car registration number. The ICO's original view was that most CCTV images would not be covered by the DPA, but their change in approach reflects the fact that systems are becoming far more commonplace and technologically advanced. Images and video recorded by CCTV surveillance must therefore be handled as 'data' in accordance with the provision of the DPA. This includes access, storage and security requirements, and the need to not keep data recorded longer than is required to fulfil the purpose of recording it in the first place.

Some of the data recorded by CCTV may constitute 'sensitive personal data' under the DPA - for example, where the images relate to the commission or alleged commission of an offence. In these circumstances, more stringent processing guidelines under the DPA must be complied with.

Subject access requests

Data subjects – i.e. those individuals about whom data relates – have the right to access such data by making a 'subject access request'. In the context of CCTV, this means that those recorded by cameras generally have a right to see a copy of any such recording unless one of the limited exemptions in the DPA applies. There are statutory time periods for a data controller (the operator of the CCTV system) to comply with such requests.

The ICO has issued two pieces of guidance to assist employers respond to subject access requests: the first, relating specifically to CCTV in the workplace, and the second, of more general application relating to all workplace 'monitoring' – see Sources of further information.

- Data Protection Act 1998.
- Human Rights Act 1998.

Sources of further information

Information Commissioner

CCTV Code of Practice: Revised Edition 2008

Employment Practices Code: November 2011

BS 7958:2009 Closed circuit television (CCTV): management and operation

Related content

- New CCTV Code of Practice
  19 Mar 2008:news analysis
- CCTV Code of Practice
  1 Jan 2008:official guidance
- Closed circuit television (CCTV). Management and operation. Code of Practice
  1 Sep 2009:official guidance
- Confidential data - shredding the evidence
  8 Sep 2009:news analysis
- Security and data protection: An update
  28 Jul 2010:documentary
- Violence at work
  :Guide
- Lone working
  :Guide
- Visitor safety
  :Guide
- Parking
  :Guide

Author

Lisa Jinks More information

Human Rights Act 1998

Under Article 8 of the Human Rights Act 1998 (the HRA) everyone has 'the right to respect for his private and family life, his home and correspondence'.

Workers' right to privacy under Article 8 may be compromised by some use of CCTV, particularly in areas where there is a legitimate expectation of privacy – toilets or private offices, for example. Employers should bear in mind the provisions of the HRA when using CCTV systems, although compliance with the DPA and various ICO Codes of Practice is likely to ensure compliance with the HRA as well.

Code of Practice for users of CCTV

The ICO published a revised CCTV Code of Practice in January 2008. It sets out the measures that should be adopted in order to ensure that a CCTV scheme complies with the DPA, as well as providing guidance on good practice.

The Code of Practice applies to most CCTV and other systems that capture images of identifiable individuals, or information relating to individuals, for specific purposes including monitoring their activities or potentially taking action against them (for example, as part of a disciplinary or criminal investigation). Note that the Code of Practice does not apply to the covert surveillance activities of law enforcement agencies or the use of conventional cameras (not CCTV) by the media or for artistic purposes such as filmmaking.

Although the Code of Practice should be considered in its entirety, Appendix 3 is specifically aimed at employers who use CCTV to monitor their workers, and supplements the guidance on monitoring employees contained in the Employment Practices Code (see below).

The full text of the Code of Practice should be considered by employers, but the main practical requirements are summarised in the following paragraphs.

Impact assessments

Employers should conduct an impact assessment before installing and using CCTV to assess whether the objectives of monitoring can be achieved by a less intrusive means.

The guidance lists a number of questions that companies should consider before installing CCTV, such as:

- What are the problems the use of CCTV will address?
- Can CCTV realistically deal with those issues?
- How will the system work in practice, and who will manage it?
- What are the views of those who will be surveyed? Can the impact on them be minimised?

Organisations must notify the ICO of the purposes for which they process data. Such notification should cover data collected through CCTV, so organisations must be clear about the purposes for which CCTV is used, and ensure the ICO is informed of these.

In some cases, it may be appropriate to install CCTV specifically for workforce monitoring, provided this is justified and properly impact-assessed. Workers should normally be made aware that they are being monitored but, in exceptional circumstances, covert monitoring may be used as part of a specific investigation (such as where there is reason to suspect criminal activity or equivalent malpractice, and covert recording is authorised by senior management having considered its effect on all workers).

Cameras and listening devices should not be installed in private areas such as toilets and private offices, except in the most exceptional circumstances where serious crime is suspected. This should only happen where there is an intention to involve the police, not where it is a purely internal disciplinary matter, and again must be authorised by senior management.

Camera positioning and signage

Cameras should be positioned in such a way that they are only able to monitor areas intended to be covered by the CCTV scheme. The operators of the equipment must be aware that they may only use the equipment in order to achieve the purpose as notified to the ICO. For example, if the aim of the CCTV is to prevent and detect crime, it should not be used for monitoring work practices or compliance with company procedures.

Clearly visible signage should be in place to inform workers that they are entering a zone where CCTV is in place (as well as anyone else who might be caught on by the CCTV). The signs should detail the identity of the person or organisation responsible for the scheme, its purpose, and details of who to contact regarding the scheme. The contact point should be available during office hours, and workers staffing the contact point should

be aware and understand the relevant policies and procedures.

Where CCTV is used to obtain evidence of criminal activity, signage may not be appropriate. However, the Code of Practice sets out tight controls over the use of CCTV in these circumstances, and employers should bear in mind that the preventative effect of CCTV is negated where no signage is used.

Image quality

Images captured by CCTV should be as clear as possible to ensure that they are effective for the purposes intended. Cameras should be properly maintained and serviced, and capable of recording with a suitable resolution. If dates and times are recorded, these should be accurate. Consideration must also be given to the physical conditions in the camera locations (e.g. infrared equipment may need to be used in poorly lit areas). Sound should not be recorded except in limited circumstances.

Images should not be retained for longer than necessary and, while they are retained, access to and security of the images must be tightly controlled in accordance with the DPA. Disclosure of images from the CCTV system must be controlled and the reasons for disclosure must be compatible with the purposes notified to the ICO. All access to or disclosure of the images should be documented - including where access is given following a subject access request.

Use of images

Images from a CCTV camera may be used as evidence in criminal and civil proceedings. However, when a company seeks to rely on CCTV evidence, consideration will have to be given to its weight. For example, where images are of poor quality, the evidence may be less reliable, and it will be important for companies to be able to authenticate any digital images presented as evidence.

Employment Practices Code

Part Three of the ICO's Employment Practices Code, (reissued in November 2011) - 'Monitoring at Work' - sets out general guidelines for employee monitoring. Employers using CCTV in the workplace must consider this Code, even where the purpose is not specifically to monitor employees – for example, CCTV systems in shops

designed to prevent shoplifting will inevitably also capture workers.

The Code stresses the need for proportionality: the adverse impact of monitoring must be justified by its benefits, whether to the employer or others. Continuous monitoring of particular workers is only likely to be justified where there are particular safety or security concerns that cannot be adequately dealt with in other, less intrusive ways. All employees and visitors to organisations should be made aware that CCTV is in operation and of the purposes for which the information will be used, subject to exceptional use of covert monitoring, discussed above.

British Standards Institution

The British Standards Institution (the BSI) has issued a Code of Practice (BS 7958:2009 *Closed circuit television (CCTV): management and operation)* to assist CCTV operators comply with the DPA (and other applicable legislation), and to ensure that CCTV evidence can be used by the police to investigate crime. The BSI's Code is particularly useful where CCTV systems are used in public places, or have a partial view of a public place.

Conclusion

Employers, and especially workplace managers responsible for CCTV, should familiarise themselves with the relevant ICO guides, as well as the underlying legislation. The main points to consider are:

- An assessment should be carried out before installing the CCTV system.
- Organisations must be clear about why CCTV is needed and what it seeks to achieve - and these purposes should be notified to the ICO.
- Clear guidelines for use should be established before the system 'goes live', which should be communicated to all staff who use, and who may be caught by, the system.
- Signs alerting people to the presence of CCTV, and containing relevant information, should normally be put in place.
- CCTV images must be handled in accordance with the requirements of the DPA, in particular those relating to storage and security.
- Organisations using CCTV should ensure they are able to comply with data subject access requests, and have a policy in place for doing so.