Sedlescombe Parish Council

CCTV Policy

Introduction

This policy is to control the management, operation, use and confidentiality of the Closed-Circuit Television (CCTV) The definition of CCTV in this policy is “equipment used to capture and store images, potentially including those of persons”.
Sedlescombe Parish Council (SPC) has 9 CCTV cameras, signs are in place to inform the public.

The use of CCTV falls within the scope of the Data Protection Act 2018 as updated by the General Data Protection Regulations (GDPR)
Human Rights Act 1998,
Regulation of Investigatory Powers Act 2000,
Surveillance Camera Code of Practice (updated March 2022) (appendix 2)

This policy will be subject to periodic review by the SPC to ensure that it continues to reflect the public interest and that it and the system meets all legislative requirements.

The CCTV Scheme is registered with the Information Commissioner
under the Terms of theData Protection Act 2018.
Registration Reference: Z6754342

SPC accepts the data protection principles as follows.
Data must be:

- used fairly, lawfully and transparently
- used for specified, explicit purposes.
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- not kept for longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

Statement of Purpose

To provide a safe and secure environment for the benefit of those who might visit, work or live in the area. The system will not be used to invade the privacy of any individual, except when carried out in accordance with the law.

The scheme will be used for the following purposes:

- to reduce the fear of crime
- to reduce the vandalism of property and to prevent, deter and detect crime and disorder
- to assist the police, the Parish Council and other Law Enforcement Agencies with identification, detection, apprehension and prosecution of offenders by examining and using retrievable evidence relating to crime, public order or contravention of bye-laws
- to deter potential offenders by publicly displaying the existence of CCTV, having cameras clearly sited that are not hidden and signs on display in areas being monitored to assist all “emergency services” to carry out their lawful duties.

Any major change that would have a significant impact on either the purpose or this policy of operation of the CCTV scheme will take place only after discussion and resolution at a Full Council meeting

Responsibilities of the Owner of the Scheme

Ownership and copyright of recorded material remains at all times the property of SPC which will deliver this Policy by delegating the responsibility of Data Controller to the Parish Clerk. Recorded material will not be sold or used for commercial purposes or for the provision of entertainment.

Management of the System

Day to day operational responsibility rests with the clerk, agreed parish councillor’s and members of the police force.
Breaches of this policy will be investigated by the Clerk and reported to SPC.
A CCTV system prevents crime largely by increasing the risk of detection and prosecution of an offender. Any relevant tape or digital evidence must be in an acceptable format for use at Court hearings. This policy must be read and understood by all persons involved in this scheme and individual copies of this policy will therefore be issued for retention. A copy will also be available for reference in the secure recording areas.

Control and Operation of the Cameras, Monitors and Systems

The following points must be understood and strictly observed by operators:
Trained operators must act with integrity and not abuse the equipment or change thepre-set criteria to compromise the privacy of an individual.

The position of cameras and monitors have been agreed following consultation with theFull Council.

No public access will be allowed to the monitors except for lawful, proper and sufficient reason, with prior approval of the clerk using the application form (appendix 1).

The Police are permitted access to tapes and prints if they have reason to believe that such access is necessary to investigate, detect or prevent crime. The police are able to visit SPC to review and confirm the Parish Council’s operation of CCTV by arrangement. The police are permitted access to tapes and prints if they have reason to believe that such access is necessary to investigate, detect or prevent crime. Any visit by the Police to view images will be

logged by the operator. Recorded images may also be made available on request to the Data Controller, whose decision to release such information is final, for the purposes of prosecution having taken into account compliance with the key objectives by the following bodies

- HM Revenue & Customs
- East Sussex County Council and or Rother District Council in pursuit of their statutory obligations
- The Health and Safety Executive
- Trading Standards

Any handheld or mobile instrument capable of linking to the main CCTV viewing system, whether used by the Police, SPC officers or volunteers, is subject to the same Policy restrictions and operational procedures as though using the main console itself.

Operators should regularly check the accuracy of the date/time displayed.

Storage and Retention of Images - Digital records should be securely stored to complywith data protection and should only be handled by the essentially minimum number ofpersons. Subject to storage capacity and imaging quality, material will be stored for a period of 30 days after which images will be overwritten and no longer available for use.

Images will not normally be supplied to the media, except on the advice of the police if itis deemed to be in the public interest. The Clerk would inform the Chairman of the Parish Council of any such emergency.

If it is decided that images will be disclosed to the media (other than in the circumstances outlined above), the images of other individuals must be disguised or blurred so that they are not readily identifiable.
If the CCTV system does not have the facilities to carry out that type of editing, an editing company may need to be used to carry it out. If an editing company is used, then the data controller must ensure that there is a contractual relationship between them and the editing company, and

- That the editing company has given appropriate guarantees regarding the security measures they take in relation to the images.
- The written contract makes it explicit that the editing company can only use the images in accordance with the instructions of the data controllers.
- The written contract makes the security guarantees provided by the editing company explicit.

As records may be required as evidence at Court, each person handling a digital record may be required to make a statement to a police officer and sign an exhibit label. Any images that are handed to a police officer should be signed for by the police officer and information logged to identify the recording and showing the officer's name and police station. The log should also show when such information is returned to the Parish Council by the police and the outcome of its use.

The Clerk will assess applications from third parties for data and will decide whether the requested access will be permitted. Disclosure of recorded images to third parties will only be made in limited and prescribed circumstances. Disclosure to third parties will be limited to the following:

- Law enforcement agencies where the images recorded would assist in a specific criminal enquiry.
- Prosecution agencies;
- Relevant legal representatives; and
- The press/media (see section on press.)

All persons requesting image(s) must complete the form at Appendix 1 and return it to the Clerk of the Council.

If access is denied the reason should be logged

Any event that requires checking of recorded data should be clearly detailed in the log book of incidents, including Crime Numbers if appropriate, and the Parish Council notified atthe next available opportunity.

Any damage to equipment or malfunction discovered by an operator should be reported immediately to the Clerk and recorded in the log. When a repair has been made, this should also be logged showing the date and time of completion.

Subject Access Requests - Any request by an individual member of the public for access to their own recorded image must be made on an Access Request Form. Forms are available by contacting the Clerk and will be submitted to the next meeting of the Parish Council for consideration and reply, normally within one calendar month. There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

Accountability

Breaches of this policy will be investigated by the Clerk and reported to the Parish Council.
A CCTV system prevents crime largely by increasing the risk of detection and prosecution of an offender. Any relevant tape or digital evidence must be in an acceptable format for use at Court hearings.
Copies of the CCTV Policy are available in accordance with the Freedom of Information Act,as with any reports that are submitted to the Parish Council providing it does not breach security needs.
The Police will be informed of the installation and provided with a copy of this CCTV Policy.

Complaints

Any written concerns or complaints regarding the use of the system will be considered by the Parish Council, in line with the existing complaints policy. Complaints must be made in writing and addressed to the clerk. Where the complaint is a third party, and the complaint or enquiry relates to someone else, the written consent of the subject data is required before any correspondence is undertaken.
All complaints will be acknowledged within seven working days, and a written response will be issued within twenty-one working days.

Adopted	Reviewed	Next Review
15th October 2019	July 2024	July 2027

Appendix 1

Data Protection Act/General Data Protection Regulation- Application for CCTV Data Access

ALL Sections must be fully completed. Attach a separate sheet if needed.

Name and address of Applicant	
Name and address of "Data Subject" – i.e. the person whose image is recorded	
If the data subject is not the person making the application, please obtain a signed consent from the data subject opposite	Data Subject signature
Please state your reasons for requesting the image.	
Date on which the requested image was taken	
Time at which the requested image was taken n.b this must be provided and be accurate to minutes	
Location of the data subject at time image was taken (e.g. which camera or cameras)	
Please indicate whether you (the applicant) will be satisfied by viewing the image only	

On receipt of a fully completed application a response will be provided within **30 days**.

Council use only	Council use only
Access Granted Y/N	Reason for granting/not granting access
Data Controllers name: Signature: Date:	

Appendix 2 Surveillance Camera Code of Practice (amended November 2021, updated March 2022)

Introduction and overview

Definitions

In this code.

- "HRA 1998" means the Human Rights Act 1998.
- "RIPA 2000" means the Regulation of Investigatory Powers Act 2000.
- "EA 2010" means the Equality Act 2010.
- "PoFA 2012" means the Protection of Freedoms Act 2012.
- "IPA 2016" means the Investigatory Powers Act 2016.
- "DPA 2018" means the Data Protection Act 2018.
- "Data protection legislation" means DPA 2018 and the UK General Data Protection Regulation.
- "ECHR" means the European Convention on Human Rights.
- "Overt surveillance" means any use of surveillance for which authority does not fall under RIPA 2000.
- "Public place" has the meaning given by Section 16(b) of the Public Order Act 1986 and is taken to include any highway and any place to which at the material time the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission.
- "Relevant authority" has the meaning given by Section 33(5) of PoFA 2012.
- "Surveillance camera systems" has the meaning given by Section 29(6) of PoFA 2012 and is taken to include: (a) closed circuit television (CCTV) or automatic number plate recognition (ANPR) systems; (b) any other systems for recording or viewing visual images for surveillance purposes; (c) any systems for storing, receiving, transmitting, processing or checking the images or information obtained by (a) or (b); (d) any other systems associated with, or otherwise connected with (a), (b) or (c)[footnote 1].
- "System Operator" – person or persons that take a decision to deploy a surveillance camera system, and/or are responsible for defining its purpose, and/or are responsible for the control of the use or processing of images or other information obtained by virtue of such system.
- "System User" – person or persons who may be employed or contracted by the system operator who have access to live or recorded images or other information obtained by virtue of such system.
- "Commissioner" is the role undertaken by the Surveillance Camera Commissioner, as set out in PoFA 2012. To encourage compliance with this code, it is the function of the Commissioner to provide information and advice on all matters within this code relevant to surveillance camera systems[footnote 2].

Background

This code of practice is issued by the Secretary of State under Sections 29 to 31 of PoFA 2012. It provides guidance on the appropriate and effective use of surveillance camera systems by relevant authorities (as defined by Section 33(5) of PoFA 2012) in England and Wales who must, under Section 33(1) of PoFA 2012, have regard to the code when exercising any functions to which the code relates. Other operators and users of surveillance camera systems in England and Wales are encouraged to adopt the code voluntarily. It is a significant step in the ongoing process of delivering the government's commitment to the 'further regulation of CCTV' which it believes is a task that is best managed in gradual and incremental stages. As understanding and application of the code increases the government may consider including other bodies as relevant authorities who will have to have regard to the code.

Purpose of this code

This code covers technology systems that are associated with, or otherwise connected with, surveillance cameras. Modern and ever-advancing surveillance camera technology provides increasing potential for the gathering and use of images and associated information. These advances vastly increase the ability and capacity to capture, store, share and analyse images, information and data. Advancements in sensor technology and artificial intelligence are developing at an ever-increasing pace, as is the ability to integrate these technologies with surveillance cameras. The overarching purpose of this code is to enable operators of surveillance camera systems to make legitimate use of available technology in a way that the public would rightly expect and to a standard that maintains public trust and confidence.

Surveillance camera systems are deployed extensively within England and Wales, and these systems form part of a complex landscape of ownership, operation and accountability. Where used appropriately, these systems are valuable tools which contribute to public safety and security, and in protecting both people and property.

The government is fully supportive of the use of overt surveillance camera systems in a public place whenever that use is: in pursuit of a legitimate aim; necessary to meet a pressing need; proportionate; effective, and compliant with any relevant legal obligations. It is the way in which technology is used that is potentially intrusive rather than the technology itself and therefore a decision to use any surveillance camera technology must be articulated clearly, documented as to the stated purpose for any deployment and be transparent, with the community being informed as to the nature of the surveillance activity being conducted and the justification for it taking place. The technical design solution for such a deployment should be proportionate to the stated purpose rather than driven by the availability of funding or technological innovation. Decisions as to the most appropriate technology should always consider the potential to meet the stated purpose without unnecessary interference with human rights; and any deployment should not continue for longer than necessary.

This code identifies clear standards and good practice without being prescriptive about the detail of how the guiding principles must be followed, or about any specific operational, technical or competency measures which a system operator should follow. This is to ensure it does not stifle innovation or fail to retain currency in an arena where technology and professional practice is expected to continue evolving.

Scope of surveillance activity to which this code applies

The code applies to the use of surveillance camera systems as defined by Section 29(6) of PoFA 2012 that operate in public places in England and Wales, regardless of whether there is any live viewing or recording of images or information or associated data. Covert surveillance by public authorities (as defined in Part II of RIPA 2000) is not covered by this code but is regulated by RIPA 2000.

Effect of the code

By virtue of Section 33(1) of PoFA 2012, a relevant authority is under a duty to have regard to this code when, in exercising any of its functions, it considers that the future deployment or continued deployment of overt surveillance camera systems to observe public places may be appropriate. This can include the operation or use of any surveillance camera systems, or the use or processing of images or other information obtained by virtue of such systems. "Having regard" to statutory guidance means that relevant authorities should take statutory guidance into account and if they decided to depart from it, they would have to have and give clear reasons for doing so[footnote 3]. It is a legitimate public expectation of relevant authorities that they are able to demonstrate how they have had regard to this code.

The duty to have regard to this code also applies when a relevant authority uses a third party to discharge relevant functions covered by this code and where it enters into partnership arrangements.

The duty to have regard does not extend to such third-party service providers or partners unless they themselves are a relevant authority. Contractual provisions or memoranda of understanding agreed after this code comes into effect with such third party service providers or partners must ensure that contractors are obliged by the terms of the contract to have regard to the code when exercising functions to which the code relates.

When used as part of civil traffic enforcement arrangements, the primary purpose of any surveillance camera system must be the safe and efficient operation of the road network by deterring motorists from contravening parking or road traffic restrictions. Any proposal to impose surveillance camera requirements as part of the conditions attached to a licence or certificate is likely to give rise to concerns about the proportionality of such an approach and will require an appropriately strong justification and must be kept under regular review. Applications in relation to licensed premises and vehicles must consider the circumstances surrounding that application and whether a requirement to have a surveillance camera system is appropriate in that case. Where there is any conflict between this code and the legislation relevant to civil enforcement functions (including any secondary legislation made or statutory guidance issued) that legislation shall apply.

A failure on the part of any person to act in accordance with any provision of this code does not of itself make that person liable to criminal or civil proceedings. This code is, however, admissible in evidence in criminal or civil proceedings, and a court or tribunal may take into account a failure by a relevant authority to have regard to the code in determining a question in any such proceedings.

Other operators of surveillance camera systems who are not defined as relevant authorities are encouraged to adopt this code and its guiding principles voluntarily and make a public commitment to doing so. Such system operators do not have to have regard to this code but it is still considered best practice.

Overview

The starting point for a system operator in achieving the most appropriate balance between public protection and individual human rights is to adopt a single set of guiding principles that are applicable to all surveillance camera systems in public places. Following these guiding principles allows a system operator to establish a clear rationale for any overt surveillance camera deployment in public places and to run any such system effectively, which helps ensure compliance with other legal duties.

To achieve this, the code sets out 12 guiding principles that should apply to all surveillance camera systems in public places. These guiding principles draw together good practice and existing legal obligations to create a regulatory framework which can be understood by system operators and the public alike. The Commissioner can provide information and advice in how the principles can be applied in various situations.

The guiding principles can be applied to numerous variations in circumstances, including changes in technology and should enable a system operator to reach informed and appropriate decisions when considering either the development or use of surveillance camera systems or the use or processing of images, information or data obtained by virtue of such systems. However, relevant authorities are encouraged to seek advice from the Commissioner and other regulators[footnote 4], before any trial or pilot of new technology is undertaken in a public place.

Guiding Principles

System operators should adopt the following 12 guiding principles:

Principle 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.

Surveillance camera systems operating in public places must always have a clearly defined purpose or purposes in pursuit of a legitimate aim and be necessary to address a pressing need (or needs). Such a legitimate aim and pressing need include national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others. That purpose (or purposes) should be capable of translation into clearly articulated objectives against which the ongoing

requirement for operation or use of the systems and any images or other information obtained can be assessed.

In assessing whether a system will meet its objectives, and in designing the appropriate technological solution to do so, a system operator should always consider the requirements of the end user of the images, particularly where the objective can be characterised as the prevention, detection and investigation of crime and the end user is likely to be the police and the criminal justice system.

A surveillance camera system should only be used in a public place for the specific purpose or purposes it was established to address. It should not be used for other purposes that would not have justified its establishment in the first place. Any proposed extension to the purposes for which a system was established and images and information are collected should be subject to consultation before any decision is taken. When using surveillance systems, you can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent from individuals, or you have a clear obligation or function set out in law.

Principle 2
The user 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.

HRA 1998 gave further effect in UK law to the rights set out in the ECHR. Some of these rights are absolute, while others are qualified or limited, meaning that it is permissible for the state to interfere with those rights if certain conditions are satisfied and the interference is proportionate. The use of surveillance cameras in public spaces places and selected sites could have the potential to impact on human rights including:

- the right to respect for private and family life (Article 8);
- freedom of thought, conscience and religion (Article 9);
- freedom of expression (Article 10);
- freedom of assembly and association (Article 11); and
- protection from discrimination (Article 14).

The right to respect for private and family life set out in Article 8 of the ECHR enshrines in law a long-held freedom enjoyed in England and Wales. People do, however, have varying and subjective expectations of privacy with one of the variables being situational. Deploying surveillance camera systems in public places where there is a particularly high expectation of privacy should only be done to address a particularly serious problem that cannot be addressed by less intrusive means. Such deployment should be subject to regular review, at least annually, to ensure it remains necessary.

Any proposed deployment that also includes audio recording in a public place is likely to require a strong justification of necessity to establish its proportionality. There is a strong presumption that a surveillance camera system must not be used to record conversations as this is highly intrusive and unlikely to be justified.

Any use of facial recognition or other biometric characteristic recognition systems needs to be clearly justified and proportionate in meeting the stated purpose and be suitably validated. It should always involve human intervention before decisions are taken that affect an individual adversely.

This principle points to the need for a data protection impact assessment (DPIA) to be undertaken whenever the development or review of a surveillance camera system is being considered to ensure that the purpose of the system is and remains justifiable, there is consultation with those most likely to be affected, and the impact on their privacy is assessed and any appropriate safeguards can be put in place. Where such an assessment follows a formal and documented process, such processes help to ensure that sound decisions are reached on implementation and on any necessary measures to safeguard against disproportionate interference with privacy.

A DPIA also helps assure compliance with obligations as data controller under the data protection legislation[footnote 5]. Comprehensive guidance on undertaking a DPIA is available from the ICO. In the case of a public authority, this also demonstrates that both the necessity and extent of any interference with Article 8 and other individual rights has been considered. Relevant authorities should satisfy themselves that a surveillance camera system does not produce unacceptable bias on any relevant ground or characteristic of the individuals whose images might reasonably be expected to be captured by it and operators should take particular account of the Public Sector Equality Duty[footnote 6].

Principle 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.

People in public places should normally be made aware whenever they are being monitored by a surveillance camera system, who is undertaking the activity and the purpose for which the associated information is to be used. This is an integral part of overt surveillance and is already a legal obligation under DPA 2018. Furthermore, such transparency supports and informs the public and forms part of the wider democratic accountability of surveillance by relevant authorities.

Responsible and legitimate surveillance is dependent upon transparency and accountability on the part of a system operator. The provision of information is the first step in transparency and is also a key mechanism of accountability. In the development or review of any surveillance camera system, proportionate consultation and engagement with the public and partners (including the police) will be an important part of assessing whether there is a legitimate aim and a pressing need, and whether the system itself is a proportionate response. Such consultation and engagement also provide an opportunity to identify any concerns and modify the proposition to strike the most appropriate balance between public protection and individual privacy.

This means ensuring effective engagement with representatives of those affected and in particular where the measure may have a disproportionate impact on a particular community. It

is important that consultation is meaningful and undertaken at a stage when there is a realistic prospect of influencing developments.

System operators should be proactive in the provision of regularly published information about the purpose, operation and effect of a system. This is consistent with the government's commitment to greater transparency on the part of public bodies.

In addition to the proactive publication of information about the stated purpose of a surveillance camera system, good practice includes considering the publication of information on the procedures and safeguards in place, impact assessments undertaken, performance statistics and other management information and any reviews or audits undertaken. Public authorities should consider including this information as part of their publication schemes under the Freedom of Information Act 2000.

This is not to imply that the exact location of surveillance cameras should always be disclosed if to do so would defeat the justified purpose identified under Principle 1.

A system operator should have an effective procedure for handling concerns and complaints from individuals and organisations about the use of surveillance camera systems. Information about complaints procedures should be made readily available to the public. Where a complaint is made and the complainant not satisfied with the response, there should be an internal review mechanism in place using a person not involved in handling the initial complaint. Complaints must be handled in a timely fashion and complainants given an indication of how long a complaint may take to handle at the outset.

Information should be provided to the complainant about any regulatory bodies who may have jurisdiction in that case such as the Information Commissioner or the Investigatory Powers Tribunal.

Where a complaint or other information comes to the attention of a relevant authority or other system operator that indicates criminal offences may have been committed in relation to a surveillance camera system, then these matters should be referred to the appropriate body, such as the police , the Independent Office for Police Conduct or the ICO for any offences under data protection legislation.

In line with government commitment towards greater transparency on the part of public authorities, a system operator should publish statistical information about the number and nature of complaints received and how these have been resolved on an annual basis at least.

The government's further commitment to 'open data' means that public authorities should consider making information available in reusable form so others can develop services based on this data. This would extend to information about surveillance camera systems.

The Commissioner has no statutory role in relation to the investigation and resolution of complaints. System operators should, however, be prepared to share information about the nature of complaints with the Commissioner on an ad hoc, and where appropriate, anonymised basis to assist in any review of the operation of this code.

Principle 4
There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

People considering the need to develop a surveillance camera system should give due consideration to the establishment of proper governance arrangements. There must be clear responsibility and accountability for such a system. It is good practice to have a designated individual responsible for the development and operation of a surveillance camera system, for ensuring there is appropriate consultation and transparency over its purpose, deployment and for reviewing how effectively it meets it purpose.

Where a system is jointly owned or jointly operated, the governance and accountability arrangements should be agreed between the partners and documented so that each of the partner organisations has clear responsibilities, with clarity over obligations and expectations and procedures for the resolution of any differences between the parties or changes of circumstance. Further guidance on this is available from the ICO.

A surveillance camera system may be used for more than one legitimate purpose. For example, one purpose might be crime prevention and detection, and another traffic management. Responsibility for each purpose may rest within different elements of a system operator's management structure but overall accountability for ensuring effective governance arrangements and facilitating effective joint working, review and audit, decision making and public engagement sits with the operator.

Principle 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.

There are significant benefits in having clear policies and procedures for the operation of any surveillance camera system. Where the operator is a relevant authority, their published policies will form part of the body of law under which they operate. Publishing and reviewing their policies and procedures will aid the effective management and use of a surveillance camera system and ensure that any legal obligations affecting the use of such a system are addressed.

A surveillance camera system operator is encouraged to follow a quality management system as a major step forward in controlling and improving their key processes. Where this is done through certification against a quality management standard, it can provide a robust operating environment with the additional benefit of reassurance for the public that the system is operated responsibly and effectively, and the likelihood of any breach of individual privacy is greatly reduced.

It is good practice that the communication of rules, policies and procedures should be done as part of the induction and ongoing professional training and development of all system users. This should maximise the likelihood of compliance by ensuring system users are competent, have relevant skills and training on the operational, technical and privacy considerations and fully understand the policies and procedures. It is a requirement of the data protection

legislation that organisations ensure the reliability of staff having access to personal data, including images and information obtained by surveillance camera systems.

Wherever there are occupational standards available which are relevant to the roles and responsibilities of their system users, a systems operator should consider the benefits and any statutory requirements associated with such occupational standards.

The Commissioner will provide advice and guidance on relevant quality management and occupational competency standards.

Wherever a surveillance camera system covers public space, a system operator should be aware of the statutory licensing requirements of the Private Security Industry Act 2001. Under these requirements, the Security Industry Authority (SIA) is charged with licensing individuals working in specific sectors of the private security industry. A public space surveillance (CCTV) licence is required when operatives are supplied under a contract for services even where that service is provided by a relevant authority. The SIA can provide more information about licencing requirements.

SIA licensing is dependent upon evidence that an individual is fit and proper to fulfil the role, and evidence of their ability to fulfil a role effectively and safely with the right skills and knowledge. There are various relevant qualifications available, and training to attain these is delivered by a range of different accredited providers.

Even where there is no statutory licensing requirement, it is good practice for a system operator to ensure that all staff who either manage or use a surveillance camera system, or use or process the images and information obtained by virtue of such systems have the necessary skills and knowledge.

Principle 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.

Images and information obtained from a surveillance camera system should not be retained for longer than necessary to fulfil the purpose for which they were obtained in the first place. This is also a requirement of data protection legislation and further guidance on this is available from the ICO.

The retention period for different surveillance camera systems will vary due to the purpose for the system and how long images and other information need to be retained so as to serve its intended purpose. It is not, therefore, possible to be prescriptive about maximum or minimum periods. Initial retention periods should be reviewed by a system operator and reset in the light of experience. A proportionate approach should always be used to inform retention periods, and these should not be based upon infrequent exceptional cases.

Although images and other information should not be kept for longer than necessary to meet the purposes for recording them, on occasions, a system operator may need to retain images

for a longer period, for example where a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation.

Principle 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.

The sharing of images and other information obtained from a surveillance camera system must be controlled and consistent with the stated purpose for which the system was established. Disclosure of images or information may be appropriate where data protection legislation makes exemptions which allow it, provided that the applicable requirements of the data protection legislation are met, or where permitted by other legislation such as the Counter Terrorism Act 2008. These exemptions include where non-disclosure would be likely to prejudice the prevention and detection of crime, and for national security purposes. Where a system operator declines a request for disclosure from a law enforcement agency, there is provision under Section 9 of and Schedule 1 to the Police and Criminal Evidence Act 1984 to seek a production order from a magistrate.

There may be other limited occasions when disclosure of images to another third party, such as a person whose property has been damaged, may be appropriate. Such requests for images or information should be approached with care and in accordance with the data protection legislation, as a wide disclosure may be an unfair intrusion into the privacy of the individuals concerned.

A system operator should have clear polices and guidelines in place to deal with any requests that are received. In particular:

- arrangements should be in place to restrict disclosure of images in a way consistent with the purpose for establishing the system.
- where images are disclosed, consideration should be given to whether images that may identify individuals need to be obscured to prevent unwarranted identification.
- those that may handle requests for disclosure should have clear guidance on the circumstances in which disclosure is appropriate.
- the method of disclosing images should be secure to ensure they are only seen by the intended recipient.
- appropriate records should be maintained.

Judgements about disclosure should be made by a system operator. They have discretion to refuse any request for information unless there is an overriding legal obligation such as a court order or information access rights. Once they have disclosed an image to another body, such as the police, then the recipient becomes responsible for their copy of that image. If the recipient is a relevant authority, it is then the recipient's responsibility to have regard to this code of practice and to comply with any other legal obligations such as data protection legislation and HRA 1998 in relation to any further disclosures.

Individuals can request images and information about themselves through a subject access request under the relevant part of the data protection legislation. Detailed guidance on this and matters such as when to withhold or obscure images of third parties caught in images is included in guidance issued by the ICO. 7.6 Requests for information from public bodies may be made under the Freedom of Information Act 2000. The ICO also produces detailed guidance on these obligations.

Principle 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.

Approved standards may apply to the system functionality, the installation and the operation and maintenance of a surveillance camera system. These are usually focused on typical CCTV installations, however there may be additional standards applicable where the system has specific advanced capability such as ANPR, video analytics or facial recognition systems, or where there is a specific deployment scenario, for example the use of body- worn video recorders.

Approved standards are available to inform good practice for the operation of surveillance camera systems, including those developed domestically by the British Standards Institute, at a European level by the Comité Européen de Normalisation Électrotechnique or at a global level by the International Electrotechnical Commission.

A system operator should consider any approved standards which appear relevant to the effective application of technology to meet the purpose of their system and take steps to secure certification against those standards. Such certification is likely to involve assessment by an independent certification body[footnote 7]. This has benefits for a system operator in that the effectiveness of a system is likely to be assured and in demonstrating to the public that suitable standards are in place and being followed.

Principle 9
Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

Putting effective security safeguards in place helps ensure the integrity of images and information should they be necessary for use as evidence in legal proceedings. This also helps to foster public confidence in system operators and how they approach the handling of images and information.

Under the data protection legislation, those operating surveillance camera systems or who use or process images and information obtained by such systems must have a clearly defined policy to control how images and information are stored and who has access to them. The use or processing of images and information should be consistent with the purpose for deployment, and images should only be used for the stated purpose for which collected.

Security extends to technical and organisational security, including cyber and physical security. There need to be measures in place to ensure appropriate security of the data and guard against unauthorised use, access or disclosure. The ICO publishes helpful guidance on achieving this in practice.

Principle 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.

A system operator should, as a matter of good governance, review and audit the continued use of a surveillance camera system on a regular basis, at least annually, together with relevant policies to ensure their system remains necessary, proportionate and effective in meeting its stated purpose(s).

As part of the regular review of the necessity, proportionality and effectiveness of a surveillance camera system, a system operator should assess whether the location of cameras remains justified in meeting the stated purpose and whether there is a case for removal or relocation.

In reviewing the continued use of a surveillance camera system, a system operator should consider undertaking an evaluation to enable comparison with alternative interventions with less risk of invading individual privacy, and different models of operation (to establish for example any requirement for 24 hour monitoring). In doing so, there should be consideration of an assessment of the future resource requirements for meeting running costs, including staffing, maintenance, and repair.

A system operator should make a summary of such a review available publicly as part of the transparency and accountability for the use and consequences of its operation.

Principle 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.

The effectiveness of a surveillance camera system will be dependent upon its capability to capture, process, analyse and store images and information at a quality which is suitable for its intended purpose. Wherever the system is used for a law enforcement purpose, it must be capable through processes, procedures and training of system users, of delivering images and information that is of evidential value to the criminal justice system. Otherwise, the end user of the images, who are likely to be the police or a law enforcement agency, will not be able to play their part effectively in meeting the intended purpose of the system – it may be difficult for an operator to argue that their purpose is to detect crime if the quality of the images produced is inadequate to support that purpose.

It is important that there are effective safeguards in place to ensure the forensic integrity of recorded images and information and its usefulness for the purpose for which it is intended to

be used. Recorded material should be stored in a way that maintains the integrity of the image and information, with particular importance attached to ensuring that meta data (e.g. time, date and location) is recorded reliably, and compression of data does not reduce its quality to an extent that it is no longer suitable for its intended purpose. This is to ensure that the rights of individuals recorded by a surveillance camera system are protected and that the material can be used as evidence in court. To do this, the medium on which the images and information are stored will be important, and access must be restricted. A record should be kept as an audit trail of how images and information are handled if they are likely to be used as exhibits for the purpose of criminal proceedings in court. Once there is no longer a clearly justifiable reason to retain the recorded images and information, they should be deleted.

It is important that digital images and other related information can similarly be shared with ease with appropriate agencies if this is envisaged when establishing a system. If this interoperability cannot be readily achieved, it may undermine the purpose for deploying the system

It is therefore essential that any digital images and information likely to be shared lawfully with other agencies and the criminal justice system are in a data format that is interoperable and can be readily exported, and then stored and analysed without any loss of forensic integrity. In particular:

- a system user should be able to export images and information from a surveillance camera system when requested.
- the export of images and information should be possible without interrupting the operation of the system.
- the exported images and information should be in a format which is interoperable and can be readily accessed and replayed.

Principle 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.

Any use of technologies such as ANPR or facial recognition systems which may rely on the accuracy of information generated elsewhere, such as databases provided by others, should not be introduced without regular assessment to ensure the underlying data is fit for purpose.

A system operator should have a clear policy to determine the inclusion of a vehicle registration number or a known individual's details on the reference database associated with such technology. A system operator should ensure that reference data is not retained for longer than necessary to fulfil the purpose for which it was originally added to a database.

When using a surveillance camera system for live facial recognition (LFR) purposes to find people on a watchlist, chief police officers should:

- set out and publish the categories of people to be included on a watchlist and the criteria that will be used in determining when and where to deploy LFR, having regard to the need only to do so for a lawful policing purpose.
- ensure that any biometric data that does not produce an alert against someone on the watchlist by the LFR system is deleted instantaneously or near-instantaneously.
- have regard to the Public Sector Equality Duty, in particular taking account of any potential adverse impact that the LFR algorithm may have on members of protected groups.
- establish an authorisation process for LFR deployments and identify the criteria by which officers are empowered to issue LFR deployment authorisations.

Footnotes

1. Excludes any camera system with relevant type approval of a prescribed device under Section 20 of the Road Traffic Offenders Act 1988 used exclusively for enforcement purposes, which captures and retains an image only when the relevant offence is detected and with no capability to be used for any surveillance purpose. For example, for the enforcement of speeding offences. ↩
2. The Commissioner's functions are set out in Section 34(2) of the 2012 Act: a) Encouraging compliance with the surveillance camera code; b) Reviewing operation of the code, and c) Providing advice about the code. ↩
3. R. (on the application of London Oratory School Governors) v Schools Adjudicator [2015]. See also R (Munjaz) v Mersey Care NHS Trust [2006] ↩
4. Where this is a forensic science activity over which the Forensic Science Regulator has oversight, the Forensic Science Code of Practice applies. ↩
5. Article 35 of the GDPR and Section 64 of DPA 2018. ↩
6. s149 of EA 2010. ↩
7. For instance, the Commissioner's third-party certification scheme. A current list of recommended standards for consideration by a system owner and operator is maintained and made available by the Commissioner. Such a list will provide detailed guidance on suitable standards and the bodies that can accredit performance against such standards. ↩