Chigwell Parish Council CCTV Draft Proposal & Policy

Adopted at the Chigwell Parish Council meeting held on (Date) minute reference xxx

Contents:

This document is to be adhered to, in conjunction with Chigwell Parish Council's Privacy Impact Assessment (Appendix D, attached) and the Surveillance Camera Commissioners Code of Practice for Councillors (Appendix E, attached).

Chigwell Parish Council CCTV Policy

1 Introduction

1.1This policy is to control the management, operation, use and confidentiality of the CCTV system owned by Chigwell Parish Council (CPC) and located within the Parish of Chigwell.

2 Legislation

2.1 The legislation relating to CCTV use is detailed in the CCTV Code of Practice issued by the Secretary of State under section 30 of the Protections of Freedoms Act 2012, published in June 2013.

The Code provides guidance on the appropriate and effective use of surveillance camera systems by relevant authorities including the Parish Council. The Code sets out 12 principles for the operation of surveillance camera systems.

Each system should:
1. Have a defined purpose and legitimate aim.
2. Not impinge on an individual's privacy or human rights.
3. Be operated transparently so people know they are being monitored.
4. Be operated with good governance.
5. Have clear policies, rules and procedures in place.
6. Store no more images/data than strictly required.
7. Have safeguards in place in relation to who can view images/data.
8. Meet relevant and approved standards.
9. Ensure images/data are stored securely.
10.Review systems regularly (at least annually).
11.Be effective in supporting law enforcement.
12. Databases used for matching purposes should be accurate and up to date.

2.2 The Information Commissioner's Office CCTV Code of Practice 2008 aims to ensure that good practice standards are adopted by those who operate CCTV. The provisions as set out within the Code remain within the current legislation as well as promoting public confidence by demonstrating that the Parish Council takes their responsibility seriously.

2.3 Chigwell Parish Council has produced a Privacy Impact Assessment in line with the Information Commissioner's code of practice, copies of which are available online and from the Parish Clerk.

2.4 The CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act 1998. The use of CCTV, and the associated images are covered by the Data Protection Act 1998. This policy outlines the parish's use of CCTV and how it complies with the Act.

2.5 All authorised operators and employees with access to images are aware of the procedures that must to be followed when accessing the recorded images. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.

3 Statement of purpose

3.1 The defined purpose of the CCTV system within Chigwell is to provide a safe and secure environment within Chigwell for the benefit of residents and visitors to the area. The pressing need which has been identified is to maintain surveillance of areas of Chigwell for the purpose of reducing or discouraging and detection of anti-social or criminal behaviour. This is a legitimate aim and has been the reason behind the installation of CCTV in many towns and villages in Britain.

The CCTV system use and effectiveness will be reviewed by the Parish Clerk and either the Finance and Governance Committee or the Community Assets Committee on a regular basis. (Minimum bi-annually)

3.2 The system will not be used to invade the privacy of any individual, except when carried out in accordance with the law. Cameras which are facing the direction of private dwellings will be electronically masked in both live and recorded images to prevent privacy being compromised. Cameras will be sited so they only capture images relevant to the purposes for which they are installed and care will be taken to ensure that reasonable privacy expectations are not violated. The Council will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act.

Cameras used will not be capable of recording sound. The cameras used will be to standard BS EN62676-4 which is the British Standard for CCYV systems in the UK. Certification of compliance with the standard will be issued by the Security Systems and Alarms Inspection Board (SSAIB).

3.3 The CCTV system will be used for the following purposes.

a) To improve community safety and reduce the fear of crime by publicly displaying the existence of CCTV within Chigwell. This will be achieved by having signage clearly sited at the entrances to the village and signage within the village informing the public of the presence of the CCTV system. It is not the intention of the Council to continuously monitor the CCTV images. (See Section 5 Proposed Methodology below)
b) To assist law enforcement agencies in the identification, detection and prosecution of offenders by allowing such agencies to examine and retrieve video evidence relating to breaches of the law.

3.4 The CCTV system will NOT be used to provide information used to support a surveillance camera system which compares data against a reference database for matching purposes such as facial recognition.

3.5 The Council complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use. The Code of Practice is published at:
https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

3.6 It is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

4 Responsibilities of the owners of the CCTV system

4.1 The Parish Council retains ownership and overall responsibility for the CCTV system. Details of responsibilities of the Parish Clerk in the operation of the CCTV system are detailed below. (See Section 5 Proposed Methodology below)

4.2 Day to day operational responsibility rests with the Clerk to the Council or in his/her absence an authorised deputy. To demonstrate the transparency with which CPC will operate the CCTV system, a contact point for access to information and for complaints will be published. Information covering the CCTV system including the complaints procedure will be published on the CPC website. A copy of the CCTV policy and procedures will be available on the Parish website and at Chigwell Cemetery as well as via the Parish Clerk.

4.3 Digital records should be securely stored to comply with the Data Protection Act. Only the Parish Clerk or a council appointed locum clerk; or an authorised Police Officer or authorised agency (appendix A) will have access to the secure hard drives containing the video images. The Parish Clerk is to keep a record of when the video storage system is accessed and at whose request.

4.4 Access to the stored images will only be made for law enforcement purposes or as part of a Subject Access Request (SAR). Details of how to make a SAR can be found in section 4.6 of this policy.

4.5 Storage of the digital images will be kept available for no more than 30 days. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded. The introduction of a CCTV system for Chigwell has been with the cooperation and advice of Essex Police and Epping Forest District Council. It is expected that any images required by law enforcement agencies will have been provided before the erasure of the images from the system. A calendar driven auto delete system will be incorporated into the Chigwell CCTV system. The Parish Clerk will on a regular basis check the accuracy of the date/time displayed on the images and ensure correctly timed erasure of images.

4.6

(a) Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act. Any request from a member of the public to view their own recorded images must be made in writing as a Subject Access Request to the Parish Clerk. The Clerk is to confirm the identity of the applicant by means of a valid passport, driving licence or similar government produced identity document. A standard fee for retrieving the images is payable, currently £10.00. The images will normally be provided within 40 days of making the request. The council will use appropriate image editing software to protect the identity of those persons shown in the image, but not covered within the Subject Access Request themselves

(b) A fee of £10 will charged per request.

(c) The Council will respond to requests within 40 calendar days of receiving the written request correct ID and fee.

(d) The Council reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

4.7 Access to the information/images stored by CPC is restricted to the Parish Clerk (or locum clerk) and members of law enforcement agencies. A receipt for Date and Time and Camera identified video images will be required by the Parish Clerk to ensure an audit trail of any images provided to authorised external agencies.

4.8 Breaches of this policy should be reported to the Parish Council in writing and will be investigated by the Parish Clerk. Where it is considered that it is the Parish Clerk who has breached the policy, the Personnel Committee will investigate any complaint of this nature.

4.9 All retained data will be stored securely.

4.10 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police or any other authorised agency.

4.11 Any requests pertaining to Chigwell Parish Council's CCTV system should be made in writing to the Parish Clerk.

5 Proposed Methodology

5.1 The system comprises a number of fixed cameras located as follows:

Brook Parade
Camera 1 = exact location including building/pole number
Camera 2 = exact location including building/pole number

Chigwell Row

Camera 1 = exact location including building/pole number
Camera 2 = exact location including building/pole number

Cemetery
Camera 1 = exact location including building/pole number
Camera 2 = exact location including building/pole number

Network video recorder/Hard Drive located within (premises) with xxxxx connectivity to xxxx. Equipment to be stored in a secure tamper proof cabinet.

5.3 Images captured by cameras located at xxx are stored within (premises) with no access to (premises) personnel.

5.4 Should an issue requiring image interrogation be identified, such as antisocial or criminal behaviour or road traffic collision:

5.5 Essex Police (EP) or relevant agency informed and advised of time & date of incident. EP may access images on xxxx premises and take copy to determine further action as required. Or see 5.8 and 5.9 below.

5.6 Parish Clerk (or locum clerk) remotely interrogates system hard drives in xxx via internet to check images.

5.7 Parish Clerk (or locum clerk) supply images to Essex Police (or other relevant police forces). EP use images to determine further action if necessary. This will consist of two disks/USB drives (one master copy, sealed) and one working copy. A data release form showing from and to dates, from and to times on the disk and the relevant camera and who the disks were handed to. A signature will be required from the representative of EP. CPC will keep this for audit purposes and proof of handover.

5.8 The data controller/ deputy should have access to details of where CCTV cameras are situated.

5.9 Complaints and enquiries regarding the operation of CCTV within Chigwell should be directed to the Parish Clerk in the first instance.

5.10 A record of verification of the time and date displayed on the system will be maintained. The time will be checked against the speaking clock (weekly). This will be kept as a log held within the parish office for inspection when necessary.

Appendix A - Authorised Agencies

Authorised agencies include:
Essex Police
Metropolitan Police
Essex Fire and Rescue Service

Appendix B

Further Information
Further information on CCTV and its use is available from the following:

CCTV Code of Practice Revised Edition 2017 (published by the Information Commissioners Office). https://ico.org.uk/

This policy has been drafted in line with the following current U.K. legislation:
Regulation of Investigatory Powers Act (RIPA) 2000
Data Protection Act 1998
Human Rights Act 1998
Protection of Freedoms Act 2012
Surveillance Camera Code of Practice 2013
Data Protection Act 2018
The Information Commissioners Office Checklist

This CCTV system and the images produced by it are controlled by Anthony Belgrave the Parish Clerk who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 1998). Chigwell Parish Council has considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of the public. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

Checked (Date)

By

Date of Next Review

Notification has been submitted to the Information Commissioner and the next renewal date recorded.

There is a named individual who is responsible for the operation of the system.

A system had been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required

Tenants will be consulted about the proposal to install CCTV equipment.

Cameras have been sited so that they provide clear images.

There are visible signs showing that CCTV is in operation.

Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.

The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.

Except for law enforcement bodies, images will not be provided to third parties

The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the Parish Clerk knows to seek advice from the Information Commissioner as soon as such a request is made.

Regular checks are carried out to ensure that the system is working properly and produces high quality images.

Appendix C

CCTV Signage
It is a requirement of the Data Protection Act 1998 to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The Council is to ensure that this requirement is fulfilled.

The CCTV sign should include the following:

That the area is covered by CCTV surveillance and pictures are recorded and the contact information of the Data Controller (Chigwell Parish clerk) is prominently displayed with the signage.

Appendix D

Chigwell Parish Council CCTV Privacy Impact Assessment (attached)

Appendix E

Surveillance Camera Commissioners Code of Practice for Councillors (attached)

Chigwell Parish Council CCTV Privacy Impact Assessment

Using CCTV can be privacy intrusive because it is capable of putting law-abiding people under surveillance and recording their movements as they go about their day to day lawful activities. Careful consideration should be given to whether to use it, or not. The fact that it is possible, affordable and has public support should not be the primary motivating factor. CPC should take into account what benefits can be gained, whether better solutions exist, and what effect it may have on individuals. The existence of a “Pressing need” should be established.

Chigwell Parish Council considers these matters objectively as part of an assessment of the scheme’s impact on people’s privacy.

There are various questions that need to be answered to successfully provide a privacy impact assessment; those questions are outlined below in a table format.

Where the system will be operated by or on behalf of a public authority, the authority will also need to consider wider human rights issues and in particular the implications of the European Convention on Human Rights, Article 8 (the right to respect for private and family life).

If this is not the case then it would not be appropriate to use CCTV

The following Privacy Impact Assessment is in two parts. Part one refers to the Data Protection Act. Part two refers to the Human Rights Act

Privacy Impact Assessment for CCTV in Chigwell

Date: May 2023

What organisations will be using the CCTV images? Who will take legal responsibility under the Data Protection Act?

Chigwell Parish Council (CPC) will be the main users of the CCTV system. CPC will be the Data Controller at the point of images being recorded. However, if these images are passed to Essex Police or any other statutory body then the legal responsibility will be transferred to that body as the data controller for the images that have been passed to them.

What is the organisation’s purpose for using CCTV? What are the issues that the system aims to address?

Chigwell Village, VIctory Hall, Chigwell Row, Chigwell Cemetery are covered by CCTV cameras provided by Chigwell Parish Council. The Council’s CCTV Service was sited in four places within the ward giving coverage of (specify in detail what is covered e.g. pedestrian crossing, cycle racks, junctions, specific areas such as playgrounds)

Essex Police in common with many UK Police Forces are willing to take images produced by CCTV cameras to assist in prosecutions.

As with many towns and villages in this country, there are examples of criminal or anti-social behaviour.

Within the last year (incidents) - provide detail and examples of the issues the systems aim to address

The CCTV has been used to identify anti social behaviour in Victory Hall car park and unauthorised access and use of the premises. It has been used to identify instances of theft and damage at Brook Parade

What are the benefits of CCTV over other methods?

CCTV is a proven tool in detecting crimes and the perpetrators. Using CCTV can significantly reduce the time and cost to the police in investigating incidents. It is also known that false allegations are made and CCTV is a useful tool in disproving some allegations. CCTV captures actual events and is not influenced by interpretation.

Can CCTV realistically deliver these benefits?

Yes, and consistently does.

Can less privacy intrusive solutions, such as improved lighting, achieve the same objectives?

There is a general agreement and belief that other solutions could help. Improved lighting throughout the night would not necessarily prevent some types of crime.

Explain why less privacy instrusive solutions may not achieve the same objectives

Members of the public will be informed that CCTV is in use by installing signs at the entrances to each area covered by CCTV for drivers and prominent signs within each area clearly visible to pedestrians detailing the scheme and its purpose, along with a contact telephone number.

Do you need images of identifiable individuals, or could the scheme use other images not capable of identifying the individual?

It is of paramount importance that the system is capable of identifying vehicles and their registration numbers if they have been involved in crime or anti- social behaviour. Footage from the system may be used in court. If the persons were not identifiable then the system would not be fit for purpose.

Will the particular equipment/system of work being considered deliver the desired benefits now and remain suitable in the future?

CPC's method of monitoring is unlikely to change. The equipment used will constantly record images from the cameras. Should an incident take place, the witness may contact the Parish Council Clerk, giving the date and time of the alleged incident. Essex Police will have access to the

recordings and may evaluate the image and if necessary, contact the perpetrator. Stored images will be available for approximately four weeks. The data is then overwritten. CPC will investigate any available technologies which will maintain a safe environment for the residents of Chigwell in order to ensure the best possible images are available

What future demands may arise for wider use of images and how will you address these?

Legislation can and does change. CPC will therefore comply with all future regulations placed upon it. As populations increase, it is realistic to assume that pressures will be put on CCTV operators to supply images to wider audiences. These include blue light services, solicitors, insurance companies and law enforcement agencies such as HMRC and the Environment Agency.

What are the views of those under surveillance?

There are some members of society both law abiding and those who are not, who have issues with being in areas covered by CCTV cameras. By abiding with current legislation, CPC aim to show that the CCTV system is only used for crime and anti-social behaviour reduction/detection purposes and those activities that assist or protect the public.

What could we do to minimise intrusion for those that may be monitored, particularly if specific concerns have been expressed?

CCTV cameras in Chigwell will not be focused on properties where privacy may be at risk of being breached in contravention of the HRA
The cameras used will not be capable of recording sound, but only video images.

Is the system established on a proper legal basis and operated in accordance with the law?

The system is to be established on a proper and legal basis and will comply with the DPA and HRA. CPC will comply with all new legislation.

Is it necessary to address a pressing need, such as public safety, crime prevention or national security?

Yes. Most town or village centres suffer instances of crime and ASB and Chigwell is no different. Installed and conspicuously operating CCTV systems throughout Chigwell will help deter or identify those involved in crime and/or committing acts considered anti-social behaviour. This information provided to Essex Police will assist in combatting crime in Chigwell.

Is it justified in the circumstances?

Yes

Is it proportionate to the problem that it is designed to deal with?

Yes. CCTV is used to detect crime and complies with the current legislation.

SURVEILLANCE CAMERA COMMISSIONER

Surveillance Camera Code of Practice
A Guide for Councillors

How well does your authority comply with the 12 guiding principles of the surveillance camera code of practice?

Executive Summary

The Protection of Freedoms Act 2012 introduced legislation governing the use of surveillance camera systems that monitor public space. This included:

- The Surveillance Camera Code of Practice (2013) and The Surveillance Camera Commissioner whose role it is to encourage compliance, review operations and provide advice about the code.
- Section 33(5) places Local Authorities on a list of 'relevant authorities' who MUST pay due regard to the code.

As a Councillor you will undoubtedly want to ensure your council is compliant with the code. The requirement to comply with the code applies to all surveillance camera systems (including CCTV, Body Worn Video and Automatic Number Plate Recognition) used by your authority, and not just those monitoring streets and town centres. It includes systems in libraries, leisure centres and town halls.

The code sets out 12 principles for the operation of surveillance camera systems. Each system should:

1. Have a defined purpose and legitimate aim
2. Not impinge on an individual's privacy or human rights
3. Be operated transparently so people know they are being monitored
4. Be operated with good governance
5. Have clear policies, rules and procedures in place
6. Store no more images/data than strictly required
7. Have safeguards in place in relation to who can view images/data
8. Meet relevant and approved standards
9. Ensure images/data are stored securely
10. Review systems regularly (at least annually)
11. Be effective in supporting law enforcement
12. Databases used for matching purposes should be accurate and up to date

This guide explains what you need to know about the surveillance camera code of practice and what it means for the camera systems your authority operates.

Furthermore, we have developed an easy to use self assessment tool which can be used to assess how closely your authority is complying with the code.

Background

The Protection of Freedoms Act 2012 introduced the regulation of public space surveillance cameras in England and Wales. As a result the surveillance camera code of practice was issued by the secretary of state under Section 30 of the Act to ensure that the use of cameras in public places is regulated and only used in pursuit of a specified purpose. The code, which came into force on 12 August 2013, seeks to balance the need for cameras in public places with individuals' right to privacy.

The code applies to the use of surveillance camera systems that operate in public places in England and Wales, regardless of whether or not there is any live viewing, or recording of images or information or associated data.

All relevant authorities must have regard to the code.

A relevant authority as defined by section 33(5) of the Protection of Freedoms Act 2012 includes all local authorities in England and Wales. This includes parish and town councils. Each council therefore has to ensure that it complies with the code when it operates any surveillance camera system that monitors public space.

Local authority use of surveillance camera

Over the last twenty-five years councils have made a considerable investment in surveillance camera systems. Often this has been due to local demand for the introduction of CCTV cameras to address concerns about crime and disorder. However some have been critical of the increasing use of CCTV and the impact this has on privacy As time and technology have progressed the ways in which surveillance cameras can be used has diversified, with some councils looking to use CCTV to address alcohol related crime and disorder and increase the safety of passengers and drivers of taxis and private hire vehicles. Others have installed systems in council facilities to reassure users, with systems monitoring libraries and leisure centres as well as being installed in council offices and town halls.

All these systems need to be operated in compliance with the code. In order to ensure it is compliant, each council needs to understand what surveillance systems it is using including public space CCTV, Automatic Number Plate Recognition (ANPR), Body Worn Videos (BWV) and Unmanned Aerial Vehicles (Drones).

To understand what your authority is using surveillance systems for; it is essential that an operational requirement is completed for each system. This will help to identify and specify the desired capabilities of the system as well as provide a basis for determining the effectiveness and suitability of the system before it is deployed. If surveillance is considered the best option, then an operational requirement will also help your authority to document the process ensuring that the proposed system is fit for purpose, has sufficient funding and public approval as well as specifying the technical requirements and a review process.

In considering whether it is compliant with the code your authority also needs to consider the circumstances in which it advocates or requires the use of surveillance cameras. It is important to note that blanket licensing policies, such as for public houses and taxis are not acceptable and there must be a pressing need and legal justification for the use of surveillance.

Issues to be addressed

Your authority needs to be aware of the number of cameras it has deployed as well as how they are deployed. It is recommended that local authorities nominate a single point of contact to oversee all the surveillance systems in the local authority and ensure that all systems are compliant with the Code.

This is vital to avoid a number of scenarios of misuse such as:

- The use of body worn cameras without appropriate training and procedures
- Use of re-deployable cameras with no operational requirement or privacy impact assessment
- Cameras with inappropriate or no signage
- The use of cameras in library, leisure centre, schools, environmental areas and waste disposal vehicles that are not compliant with the code of practice and the Data Protection Act
- No single point of contact for all local authority public space surveillance

There are a number of principles guiding the use of surveillance systems that your authority needs to consider when dealing with requests for additional cameras or systems in your area.

The Surveillance Camera Code of Practice

The code of practice is made up of 12 guiding principles and it is important that these principles are considered when using a surveillance system within a public space as defined by the code.

These principles should be considered before installing a new camera or camera system and also be applied to surveillance systems that have already been set up. To monitor compliance, if your council is yet to do so, you should ask your officers whether they have reviewed all the surveillance systems in your area. This will help you to identify what systems your authority has and why it has them.

The office of the surveillance camera commissioner has produced a simple self assessment tool that will enable your council to assess its level of compliance to the twelve guiding principles. It is important that your council identifies all surveillance systems it uses and completes the self assessment tool for each system.

Adhering to the code of practice will ensure that the use of surveillance systems in your authority is legal and being used in response to a pressing need. It will also assist in ensuring that the public space surveillance is effective, proportionate and transparent.
The self assessment tool can be found at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/372082/Self_assessment_tool_v3_WEB.pdf

The principles

Principles you need to consider regarding the surveillance systems used in your jurisdiction

Principle one

Purpose: 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.

It is important that any surveillance systems in your council have clearly defined purposes, so please check to make sure that the purposes are legitimate and have been clearly written down.

Questions your officers should consider about any system include:

- What is the system for?
- Does it have clear objectives?
- Is the system reviewed frequently against its stated purpose?
- Has it been used for anything other than its original purpose?
- If yes, what was the justification?

Principle two

Privacy: 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.

The use of any form of surveillance will have an impact on individual's privacy and rights under the Human Rights Act. As a result it is essential that this is considered in detail before a system is installed. A privacy impact assessment should be conducted in order to consider any impact the surveillance system will have on individuals and groups in the society and this impact must be proportional and justifiable. When considering plans and proposals to install new systems you should ask your officers:

- Is surveillance the best solution for the problem they are seeking to address?
- Have they conducted a privacy impact assessment?
- If yes, has it been published?
- Have they taken necessary steps to reduce any impact on individual's privacy? (such as the use of privacy zones)

Principle three

Transparency: 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 a public place should be made aware that they are being monitored therefore there must be signs in place informing them that they are in a surveillance zone. The sign should have basic information including contact details for the owner of the system.

In order to ensure transparency, as much information about the system as possible should be published, this could include the number of cameras, purpose, crime statistics and consultation outcomes. In summary:

- Does your council have adequate signage?
- Has your council adequately engaged with those affected by the cameras?
- Does your authority publish information regarding the cameras on its website?
- Does your council have a procedure for handling concerns and complaints about the use of the surveillance systems?
- Are the public aware of how to make a complaint?

Principle four

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

There must be established governance arrangements for the surveillance systems in your council. If a system is jointly owned then the lines of responsibilities must be agreed and made known to all relevant parties. Questions to consider include:

- Who owns the system?
- Is the system jointly owned?
- Are there clear established lines of responsibilities
- Does the council have a designated individual responsible for the development and operation of the system?
- Are all staff aware of their responsibilities?
- Are all staff aware of the lines of responsibilities

Principle five

Rules, Policies and Procedures: 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.

The existence of clear policies and procedures are essential to meet any legal obligations regarding the use of the surveillance system such as compliance with the Data Protection Act. Once policies are in place they should be communicated to all staff and in particular to new staff at the induction stage.

You should find out whether your operators are required to have a Security Industry Authority (SIA) licence. Information on licensing requirements can be found on the SIA website at http://www.sia.homeoffice.gov.uk/Pages/licensing.aspx

Things to consider include:

- Does your council have clear policies in place?
- Have they been communicated to all staff and are they clearly accessible?
- Has your authority considered qualifications relevant to the role of the system users?
- Has your council considered the use of an SIA licence for its operators?

- How does your council ensure that its system users have the relevant skills and knowledge for the job?

Principle six

Storage: 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.

It is important that images and information from the surveillance camera systems are not kept for longer than is necessary to accomplish the original purpose for which they were installed. Things to consider include:

- How long are the images and information retained?
- Does your council have a policy on retention for law enforcement purposes?
- How does your council ensure that law enforcement agencies are aware of the retention policy?
- Is there an audit process to ensure that images and information are not stored for longer than necessary?

Principle seven

Access: 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.

It is essential to ensure that there is limited and restricted access to the stored information. As a result there should be clear rules on to whom and when access is allowed. An operator must have clear policies and guidelines to deal with any requests to view information.

As individuals are entitled to a copy of images of themselves, it is essential to have a policy on place to deal with subject access requests.

Things to ask should include:

- Does your council have a policy in place on who has access to the stored information?
- What is your council's policy on disclosure of information? Are all staff aware of these policies
- What checks are in place to ensure that these policies and procedures are followed?

Principle eight

Approved Standards: 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.

It is important to consider any approved standards for the installed system. This could be for the functioning, installation, operation and maintenance of the system. This is particularly important when there is a specific deployment requirement such as the use of body worn cameras.

A list of approved standards is available on the Surveillance Camera Commissioner's website at https://www.gov.uk/recommended-standards-for-the-cctv-industry

Things to consider include:

- What approved operational, technical and competency standards relevant to a surveillance system and its purpose does your council's system(s) meet?
- How does your council ensure that these standards are followed appropriately?
- What steps are in place to secure certification against the approved standards?
- Have your officers considered certification against the surveillance camera code of practice?

Principle nine

Security and Safeguards: Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

It is essential to have effective safeguards to help ensure the integrity of the images and information particular if they are necessary as evidence in court proceedings. It is important to ask the following:

- What security safeguards does your council have in place to ensure the integrity of images and information?
- If the system is connected across an organisational network or intranet, do sufficient controls and safeguards exist?
- What is the specified purpose for which the information are being used and accessed and is this consistent with the stated purposes?
- Does your council have preventative measures in place to guard against misuse of information and images?
- Are your council's procedures and instructions and/or guidelines regarding the storage, use and access of surveillance system information documented?

Principle ten

Review and Audits: 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.

It is good practice to review the continued use of a surveillance camera system on a regular basis, at least annually, to ensure that it remains necessary, proportionate and effective in meeting its specified purpose.

- How frequently is the system reviewed? (recommended to be at least annually)
- Does your council have a review process that shows its system(s) still addresses the needs and delivers the benefits that justify its use?
- Has your council identified any cameras that do not remain justified in meeting the stated purpose(s)?
- Have your officers conducted an evaluation in order to compare alternative interventions to surveillance cameras?
- Is it cost effective to continue running your council's surveillance camera system?

Principle eleven

Support Law Enforcement: 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 your council's system is dependent on its ability to capture, process, analyse and store images and information. This is particularly important if the purpose of your authority's system includes the prevention, detection and investigation of crime. If this is the case your council's system should be capable of producing images and information that are suitable for the criminal judicial system. Things to consider include:

- Are the images and information produced by your authority's system of a suitable quality for the criminal justice system to use without enhancement?
- During the production of the operational requirement for your council's system, what stakeholder engagement was carried out or guidance followed to ensure exported data would meet the quality required for it to be used for evidential purposes?
- Does your council have safeguards in place to ensure the forensic integrity of the images and information including a complete audit trail?
- Does your council have a policy on data storage, security and deletion?
- Is the information stored in a format that is easily exportable?
- Does the storage ensure the integrity and quality of original recording and the meta data?

Principle twelve

Reference Database: 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.

If your council uses specific technologies such as ANPR or facial recognition, you should satisfy yourself that the underlying data is accurate and fit for purpose. It is important to consider the following questions:

- Does your council use any specialist technology such as ANPR, facial recognition, Body Worn Video (BWV) or remotely operated vehicles (Drones)?
- Does your council have a policy in place to ensure that the information contained on its database is accurate and up to date?
- Does your council have a procedure for deciding when and whether an individual or vehicle should be included in a reference database?
- What policies are in place to determine how long information remains in the reference database?
- Are all staff aware of when surveillance becomes covert surveillance under the Regulation of Investigatory Powers Act (RIPA) 2000?