SURVEILLANCE CAMERA COMMISSIONER

Self assessment tool

How well does your organisation comply with the 12 guiding principles of the surveillance camera code of practice? Complete this easy to use self assessment tool to find out if you do.

Using this tool

This self assessment tool will help you and your organisation identify if you're complying with the principles in the code. It should be completed in conjunction with the surveillance camera code of practice. The tool will help you show how well you comply with each principle. It is possible to be largely compliant with some principles and to fall short against others. As a result you will note that at the end of the questions against each principle there is a space to include an action plan. This is to enable you to put actions in place over the next year to improve your compliance to that principle. These boxes can also be used to make a note of what evidence you could produce if required to show your compliance to that principle.

The document contains a combination of open and closed questions. For the open questions there is a limit on how much you can write, so please feel free to include any additional notes as an annex to the document – there are additional blank pages at the end of the tool.

We do not want you to send the self assessment response to us. However, in the interest of transparency we encourage you to publish the self assessment on your website.

The self assessment is for you to satisfy yourself and those that you surveille that you meet the principles and identify any additional work to show compliance.

We would like you to let us know that you have completed this document as this will enable us to understand the level of uptake. Also please let us know if you will be interested in working towards certification against the surveillance camera code of practice in the near future or just be added to our mailing list.

This is the first edition of the self assessment tool which will evolve over time. Please forward any feedback to scc@sccommissioner.gsi.gov.uk

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.

1. Have you translated principle 1 into clear objectives? ☑ Yes ☐ No

If so what are they?

CCTV is used for the prevention and detection of Crime and Disorder, to improve public safety and protect the rights and freedom of others.

The Council uses ANPR systems in some Council owned car parks for charging purposes with customers being aware that ANPR operates and consenting by choosing to use the car parks. The legitimate aim is the protection of the rights and freedoms of others by ensuring that parking is available on a rolling basis to the public, when needed, and for the detection of crime and disorder as incidents of crime do occur in car parks

2. Do you regularly review the system and assess against the objectives? ☑ Yes ☐ No

3. Have you considered the requirement of the end user? ☑ Yes ☐ No

4. Is the system being used for any other purpose other than those specified? ☐ Yes ☑ No

If so please explain

5. Have you identified any areas where further action is required more fully conform with the requirements of Principle 1?

Action plan

Principle 2

The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

1.	Do you review your system annually?	☑ Yes	☐ No
2.	Have you conducted a privacy impact assessment? (The ICO has produced a PIA code of practice and the SCC has a template you can use if required)	☑ Yes	☐ No
3.	Do you publish your privacy impact assessment and annual review?	☑ Yes	☐ No

4. Have you identified any areas where further action is required to more fully conform with the requirements of Principle 2?

Action plan

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.

1.	Does signage exist highlighting the use of surveillance cameras?	☑ Yes	☐ No
2.	Does the signage highlight the point of contact?	☑ Yes	☐ No
3.	Has there been proportionate consultation and engagement with the public and partners to establish that there is a legitimate aim and a pressing need for the surveillance camera system?	☑ Yes	☐ No
4.	Is the surveillance system a proportionate response?	☑ Yes	☐ No

5.	Does your publication of information include the procedures and safeguards that are in place, impact assessments undertaken, performance statistics and other management information?	☑ Yes	☐ No
6.	Do you have a complaints procedure in place?	☑ Yes	☐ No
7.	Do you make the public aware of how to escalate complaints?	☑ Yes	☐ No
8.	Is there a defined time scale for acknowledging and responding to complaints and is this conveyed to the complainant at the outset?	☑ Yes	☐ No
9.	Do you publish the number and nature of complains received?	☑ Yes	☐ No

10. Have you identified any areas where further action is required to more fully conform with the requirements of Principle 3?

Action plan

Principle 4

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

1. What arrangements are in place to provide clear responsibility and accountability?

Wycombe District Council is responsible for the provision of the CCTV monitoring equipment and the transfer of the data through secure network to other locations as it provide a monitoring service for Chiltern District Council and Beaconsfield Town Council.
Wycombe District Council CCTV control room who is responsible for the monitoring and recording of data and alerting Thames Valley Police to an incident.
Thames Valley Police are responsible for requesting the viewing and gathering of evidence required to prosecute a crime.

Data controller: Wycombe District CCTV ----Wycombe District Council
Chiltern District CCTV ---- Joint control /ownership of data with WDC
Beaconsfield Town Council --- Joint control / ownership of data with WDC

2. Are all staff aware of their responsibilities? ☑ Yes ☐ No

3. Please explain how you ensure the lines of responsibility are adhered to.

Agreements are currently in place between the various authorities and staff at Wycombe District Council are trained in the collection, recording and monitoring systems.

4. If jointly owned, is it clear what each partner organisation is responsible for and what the individual obligations are? ☑ Yes ☐ No

5. Have you identified any areas where further action is required to more fully conform with the requirements of Principle 4?

Action plan

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.

1. Do you have clear policies and procedures which help ensure that any legal obligations affecting the use of such a system are addressed? ☑ Yes ☐ No

If so please specify.

Code of Practice and operating procedures are in place to ensure that all legislations are complied with.
Any Legal issue is passed on to appropriate expert in the Council's Legal team for advice and/or action. Other issues are covered by the Council's Complaint's Procedure.

2. Do you follow a quality management system? ☑ Yes ☐ No

If so please specify.

BSI EN ISO9001:2008 (to be amended and updated to ISO9001:2015 during early 2018)

3. Are the rules, policies and procedures part of an induction process for all staff? ☑ Yes ☐ No

4. How do you ensure that all system users remain up to date and efficient with relevant operational, technical, privacy considerations, policies and procedures?

Regular reviews of internal procedure, visiting exhibitions, attending seminar and attending appropriate courses. Also keeping up to date by reading trade magazines.
Regular survey of CCTV coverage areas.

5. Have you considered qualifications relevant to the role of the system users, such as the National Occupational Standard for CCTV operations or other similar? ☑ Yes ☐ No

6. If so, have any of your system users undertaken any occupational standards to date? ☑ Yes ☐ No

7. Do your system users require SIA licenses? ☑ Yes ☐ No
(Please see SIA website: www.sia.homeoffice.gov.uk)

8. If staff do not need a license, how do you ensure they have the necessary skills and knowledge to use or manage the surveillance system?

All staff are SIA licensed.

9. Have you identified any areas where further action is required to more fully conform with the requirements of Principle 5?

Action plan

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.

1. On what basis are images retained and for how long?

The images are retained for 31 days (national norm for LA). This gives the police, other enforcement and the general public sufficient time to request footage. The system automatically delete images older than 31 days.

2. Do you have an auditable process for reviewing images and managing their retention? ☑ Yes ☐ No

3. Are there any time constraints in the event of the enforcement agency not taking advantage of the opportunity to view the retained images? ☑ Yes ☐ No

4. Are there any time constraints which might affect external parties from viewing the images? ☑ Yes ☐ No

5. Do you quarantine all relevant information and images relating to a reported incident until such time as the incident is resolved and/or all the information and images have been passed on to official third parties? ☑ Yes ☐ No

6. Have you identified any areas where further action is required to more fully conform with the requirements of Principle 6?

Action plan

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.

1. Do you have a policy on who has access to the stored information? ☑ Yes ☐ No

2. Do you have a policy on disclosure of information? ☑ Yes ☐ No

3. What checks do you have in place to ensure that the disclosure policy is followed?

Internal Code of Practice. Data Protection Act and the Freedom Of Information Act are adhered to and only only the CCTV Operations Manager deals with enquiries from non-enforcement agencies. Regular audits and checklist which forms part of the ISO9001:2008 quality management system.

4. Have you identified any areas where further action is required to more fully conform with the requirements of Principle 7?

Action plan

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.

1. What approved operational, technical and competency standards relevant to a surveillance system and its purpose does your system meet?

ISO9001:2008, the Code of Practice and the CCTV and Surveillance Codes of Practice are followed and complied with.
Operator are trained to BTEC level and are sent on refresher course every 3 years. All other CCTV legislation are followed. Internal performance reports are produced quarterly and yearly.

2. How do you ensure that these standards are followed appropriately?

Internal checklists and audits, internal and external (BSI) - part of the ISO9001:2008 system.

3. What steps are in place to secure certification against the approved standards?

As above

4. Have you identified any areas where further action is required to more fully conform with the requirements of Principle 8?

Action plan

Principle 9

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

1. What security safeguards do you have in place to ensure the integrity of images and information?

Secured premises, system user name and password protected . An Information Security Policy is followed to ensure safeguarding and integrity is maintained. Also, system logs provide a full audit trail of camera used and data copied as well as paper based logs.

2. If the system is connected across an organizational network or intranet, do sufficient controls and safeguards exist? ☑ Yes ☐ No

3. What is the specified purpose for which the information are being used and accessed and is this consistent with the stated purposes?

Yes, for CCTV to allow police control room operators and senior officers in the police control room to view serious incident in progress and advise officers on scene. Viewing access is controlled by the CCTV Control room operators.

For ANPR the information is used to calculate parking periods but not as evidence of enforcement. Also, this data may also be used in crime detection e.g. when a motor vehicle is stolen from a ANPR controlled car park.

4. Do you have preventative measures in place to guard against misuse of information and images? ☑ Yes ☐ No

5. Are your procedures and instructions and/or guidelines regarding the storage, use and access of surveillance system information documented? ☑ Yes ☐ No

6. Have you identified any areas where further action is required to more fully conform with the requirements of Principle 9?

Action plan

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.

1. Does your system have a review process that shows it still addresses the needs and delivers the benefits that justify its use? ☑ Yes ☐ No

2. Have you identified any cameras that do not remain justified in meeting the stated purpose(s)? ☑ Yes ☐ No

3. Have you conducted an evaluation in order to compare alternative interventions to surveillance cameras? ☑ Yes ☐ No

If so please provide brief details.

Additional street lighting in certain areas but there are cost restraint which does not allow this.

4. Is it cost effective to continue running your surveillance camera system? ☑ Yes ☐ No

5. Have you identified any areas where further action is required to more fully conform with the requirements of Principle 10?

Action plan

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.

1. Are the images and information produced by your system of a suitable quality for the criminal justice system to use without enhancement? ☑ Yes ☐ No

2. During the production of the operational requirement for your 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?

Specialist consultant provided guidance and the latest equipment available was used.

3. Do you have safeguards in place to ensure the forensic integrity of the images and information including a complete audit trail? ☑ Yes ☐ No

4. Do you have a policy on data storage, security and deletion? ☑ Yes ☐ No

5. Is the information stored in a format that is easily exportable? ☑ Yes ☐ No

6. Does the storage ensure the integrity and quality of original recording and the meta data? ☑ Yes ☐ No

7. Have you identified any areas where further action is required to more fully conform with the requirements of Principle 11?

Action plan

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.

1. Do you use any specialist technology such as ANPR, facial recognition, Body Worn Video (BWV) or remotely operated vehicles (Drones)? ☑ Yes ☐ No

If so, please specify.

Facial recognition, Body Worn Video and Drones are not used used by the Council.

ANPR is used in some of the Council's car park to clock parking period for the production of ticket. ANPR can also be used in crime detection e.g. when a motor vehicle is stolen from a ANPR controlled car park.

2. Do you have a policy in place to ensure that the information contained on your database is accurate and up to date? ☑ Yes ☐ No

3. Do you have a procedure for deciding when and whether an individual or vehicle should be included in a reference database? ☑ Yes ☐ No

4. What policies are in place to determine how long information remains in the reference database?

The Council's Data Protection Protocol and Retention and Disposal of Documents Schedule is followed in relation to any personal data held on the Council's systems.

5. Are all staff aware of when surveillance becomes covert surveillance under the Regulation of Investigatory Powers Act (RIPA) 2000? ☑ Yes ☐ No

6. Have you identified any areas where further action is required to more fully conform with the requirements of Principle 12?

Action plan

Additional Information

Additional Information

Additional Information