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 has been prepared by the Surveillance Camera Commissioner (SCC) to help you and your organisation identify if you're complying with the Surveillance Camera Code of Practice (the Code). It should be completed in conjunction with the Code, and can help to show you how well you comply with each of its 12 guiding principles.

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 so you can 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 template contains a combination of open and closed questions. For the open questions, there is a limit on how much you can write within the template, 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 to help you to do so.

Remember that your organisation may operate more than one surveillance camera system, with a scope that extends across several purposes and many geographical locations. So, before you start clarify the scope of the system(s) you propose to self assess for compliance against the Code.

Is this tool for me?

The self assessment tool is aimed primarily at relevant authorities under Section 33 of the Protection of Freedoms Act 2012 who have a statutory duty to have regard to the guidance in the Code. In general terms, this means local authorities and the police in England and Wales.

If you work within any other organisation that operates surveillance camera systems you are free to adopt and follow the principles of the Code on a voluntary basis. If you decide to do so, then using this tool will be of benefit to you.

As a relevant authority under Section 33, if you are considering the deployment of a new surveillance camera system, or considering extending the purposes for which you use an existing system, you may find the more detailed three stage passport to compliance tool a valuable planning tool. It can guide you through the relevant principles within the Code and inform you of the necessary stages when planning, implementing and operating a surveillance camera system to ensure it complies with the Code.

If you are from any other organisation operating a surveillance camera system you may find this template useful in reviewing your use of surveillance, or may want to use other SCC online tools such as the Data Protection Impact Assessment guidance or the Buyers Toolkit to help decide whether your surveillance is necessary, lawful and effective.

What should I do next?

The self assessment is for you to satisfy yourself and the subjects of your surveillance that you meet the 12 principles and to identify any additional work necessary to show compliance. Think about realistic timescales for completion of your action plans, with a view to achieving full compliance with the Code before undertaking your next annual review.

The SCC does not want you to submit your completed self assessment response to him. However, in the interest of transparency he encourages you to publish the completed self assessment tool template on your website.

A completed self assessment is also a positive step towards third party certification against the Code.

Email the SCC at scc@sccommissioner.gsi.gov.uk to let us know when you have completed this template as this will enable us to understand the level of uptake. We would also appreciate your comments and feedback on the user experience with this template. Please let us know if you are interested in working towards third party certification against the Code in the near future, or would like to be added to our mailing list.

Name of organisation	South Tyneside Council
Scope of surveillance camera system	Although the CCTV Unit monitor a number of different CCTV schemes this is obly in relation to the Public space surveillance within the borough.
Senior Responsible Officer	Andrew Bailey
Position within organisation	Acting lead Officer for Community Safety
Signature	
Date of sign off	14/12/18

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. What is the problem you face and have you defined a purpose in trying to solve it? Have you set objectives in a written statement of need?

The function of CCTV operations within South Tyneside Council is to proactively monitor public places by use of an expanding public space CCTV network. This monitoring is designed to assist with the prevention and detection of crime by facilitating the gathering and preserving of video evidence for use in criminal court proceedings.

In order to achieve this, the Council operates a professionally run and operated CCTV control centre that uses both analogue and digital recording media to capture and store video footage. The Council participates in CCTV Partnership with the following partner organisations:

Northumbria Police, British Transport Police, NEXUS, Sunderland City Council, Gateshead MBC. Newcastle City Council and North Tyneside Council.

The continued operation and success of all CCTV systems are dependent on the continued consensus of the public to allow public space CCTV monitoring. Therefore in order to preserve this consensus the control room operations are maintained in compliance with the ICO (Information Commissioner's Office) COP (Code of Practice) for the use of CCTV in Public Space.

South Tyneside Council introduced the CCTV for the following purpose:

-To deter and detect criminal activity.

-To identify suspects.

-To gather evidence.

-To gather intelligence on suspects (Under the Regulation of Investigatory Powers Act)

-To aid in prosecutions.

-To monitor anti-social behaviour and acts or events which endanger the public and Employees' health and safety.

-To assist the emergency services.

-To assist in Traffic Management.

The system at no time will be used to look into private residences or private premises unless a justified need is identified. No sound recording facility is used in any public area.

The Council is committed to complying with the Surveillance Camera Code of Practice, the

Data Protection Act 2018 and the Human Rights Act 1998. The Council is committed to ensuring that the public is kept informed and consulted on future developments of the CCTV system.

2. What is the lawful basis for your use of surveillance?

Crime and disorder Act 1998 sect 17 Duty to consider crime and disorder implications.

(1)Without prejudice to any other obligation imposed on it, it shall be the duty of each authority to which this section applies to exercise its various functions with due regard to the likely effect of the exercise of those functions on, and the need to do all that it reasonably can to prevent,

[F1(a)crime and disorder in its area (including anti-social and other behaviour adversely affecting the local environment); and

(b)the misuse of drugs, alcohol and other substances in its area][F2; and

(c)re-offending in its area]

3. What is your justification for surveillance being necessary and proportionate?

Is it necessary and proportionate to the CCTV is used to detect crime and complies with theproblem that it is current legislation A full privacy impact assessment has been carried out.

4. Is the system being used for any other purpose other than those specified? If so please explain. ☐ Yes ☒ No

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

Action Plan

No

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. Has your organisation paid a registration fee to the Information Commissioner's Office and informed them of the appointment of a Data Protection Officer (DPO) who reports to the highest management level within the organisation?

☒ Yes ☐ No

2. Are you able to document that any use of automatic facial recognition software or any other biometric characteristic recognition systems is necessary and proportionate in meeting your stated purpose?

☒ Yes ☐ No

3. Have you carried out a data protection impact assessment, and were you and your DPO able to sign off that privacy risks had been mitigated adequately?

☐ Yes ☒ No

Before May 2018 the requirement was to complete a privacy impact assessment; this has been replaced by a data protection impact assessment. There is a surveillance camera specific template on the Surveillance Camera Commissioner's website: https://www.gov.uk/government/publications/privacy-impact-assessments-for-surveillance-cameras

4. Do you update your data protection impact assessment regularly and whenever fundamental changes are made to your system?

☐ Yes ☒ No

5. How have you documented any decision that a data protection impact assessment is not necessary for your surveillance activities together with the supporting rationale?

Will be reviewing the old Privacy impact assessment publicshed in Feb 2018 in Feb 2019 and replacing with the new Data protection Risk Assessment at this point.

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

☒ Yes ☐ No

Action Plan

See above. New Data Protection Assessment to be completed in Feb 2019.

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.

7. Has there been proportionate consultation and engagement with the public and partners to assess whether there is a legitimate aim and a pressing need for the system? ☒ Yes ☐ No

8. Does your Privacy Notice signage highlight the use of a surveillance camera system and the purpose for which it captures images? ☒ Yes ☐ No

9. Does your signage state who operates the system and include a point of contact for further information? ☒ Yes ☐ No

10. If your surveillance camera systems use body worn cameras, do you inform those present that images and sound are being recorded whenever such a camera is activated? ☒ Yes ☐ No

11. What are your procedures for handling any concerns or complaints?

All complaints are recorded omn the corporate feedback system administered by the Information Team. Strict timescales and escalation procedures are in place. See attached website link.
https://www.southtyneside.gov.uk/article/38286/Complaints

12. Have you identified any areas where action is required to conform more fully with the requirements of Principle 3? ☐ Yes ☒ No

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.

13. What governance arrangements are in place?

Codes of practice in place and regularly reviewed. See attached links.
https://www.southtyneside.gov.uk/article/35109/Disclosure-of-CCTV-images.
https://www.southtyneside.gov.uk/article/35108/CCTV-and-data-protection.

14. Do your governance arrangements include a senior responsible officer? ☒ Yes ☐ No

15. Have you appointed a single point of contact within your governance arrangements, and what steps have you taken to publicise the role and contact details? ☐ Yes ☒ No

Guidance on single point of contact: https://www.gov.uk/government/publications/introducing-a-single-point-of-contact-guidance-for-local-authorities/introducing-a-single-point-of-contact

16. Are all staff aware of the roles and responsibilities relating to the surveillance camera system, including their own? ☒ Yes ☐ No

17. How do you ensure the lines of responsibility are always followed?

Through our codes of practice and regular training.

18. If the surveillance camera system is jointly owned or jointly operated, is it clear what each partner organisation is responsible for and what the individual obligations are? ☒ Yes ☐ No

19. Have you identified any areas where action is required to conform more fully with the requirements of Principle 4? ☒ Yes ☐ No

Action Plan

Although a report has gobe through on a Single Point of Contact and agreed in principle du e to capacity issues and the vast amount of systems in place within the council, this has not been progressed at present. This will be reviewed in 2019.

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.

20. Do you have clear policies and procedures in place to support the lawful operation of your surveillance camera system? If so, please specify.

☒ Yes ☐ No

21. Are the rules, policies and procedures part of an induction process for all staff?

☒ Yes ☐ No

22. How do you ensure continued competence of system users especially relating to relevant operational, technical, privacy considerations, policies and procedures?

Refresher training carried out regulary.

23. Have you considered occupational standards relevant to the role of the system users, such as National Occupational Standard for CCTV operations or other similar?

☐ Yes ☒ No

24. If so, how many of your system users have undertaken any occupational standards to date?

25. Do you and your system users require Security Industry Authority (SIA) licences?

☒ Yes ☐ No

26. If your system users do not need an SIA licence, how do you ensure they have the necessary skills and knowledge to use or manage the surveillance system?

N/A

27. If you deploy body worn cameras, what are your written instructions as to when it is appropriate to activate BWV recording and when not?

An extract of the Body Warn Camera Codes of Practice for the Community Wardens.

3.3 Confidentiality

Camera and camera footage must never be used for personal use or gain. All data, digitally or manually stored media, still photographs or any piece of intelligence supplied by any agency must not be removed from the Community Warden Offices by any person other

than relevant officer with the expressed permission. Officers are in a position of extreme trust and must never divulge information to any third party.

Staff are required to attach the body cams to the front windscreen of the Community Warden vehicle using the appropriate holder when they are carrying out mobile patrols. When officers are called to an incident or come across one, they are required to switch on the camera and start recording for evidential purposes. When alighting the vehicle, the officer should wear a body cam on attendance at an incident and again start recording.

The officer will notify the base if any evidential footage is obtained. This will be recorded on the database and the incident report.

4.2 Downloading of footage.

On completion of a shift or sooner if required, the officer should return the body cams to the office for the base control to download and delete the footage from the camera.

The footage is retained on the NAS5 server within the Community Wardens Folder within a folder called Community Warden CCTV Footage. This ensures that any footage is backed up and reduces the chance of any accidental deletion or loss of images.

Any evidential footage is retained for 28 days and in that time it can be shared with other relevant partner agencies for evidential purposes.

4.3 Log book recording.

On any requests for footage, a disc is produced for the agency and footage deleted from the server.

A log of this is made and recorded in the review and downloading footage log book.

Once an agency requests and receives a disc it becomes their responsibility.

28. If you deploy surveillance cameras using drones, have you obtained either Standard Permission or Non-Standard Permission from the Civil Aviation Authority and what is your CAA SUA Operator ID Number?

☐ Yes ☐ No

N/A

29. Have you identified any areas where action is required to conform more fully with the requirements of Principle 5? ☒ Yes ☐ No

Action Plan

Revise Privacy Impact Assessment to new Data protectiion Act Risk Assesment for Body Worn Vide in 2019.

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.

30. How long is the period for which you routinely retain images and information, and please explain why this period is proportionate to the purpose for which they were captured?

South Tyneside Council is registered with the Information Commissioner's Office (ICO) for its CCTV operations and will abide by the constraints laid down within the Data Protection Act 2018 and the ICO's CCTV Code of Practice. CCTV recordings are retained for a maximum of 30 days unless there is a justification to retain longer.

31. What arrangements are in place for the automated deletion of images?

The Video recorders are set to overwrite of prescribed time period unless there is a justification to retain..

BWV Footage is adited and any footage stored over this time is deleted unless there is a justification to retain.

32. When it is necessary to retain images for longer than your routine retention period, are those images then subject to regular review? ☒ Yes ☐ No

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

34. 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 the enforcement agencies? ☐ Yes ☒ No

35. Have you identified any areas where action is required to conform more fully with the requirements of Principle 6? ☐ Yes ☒ No

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.

36. How do you decide who has access to the images and information retained by your surveillance camera system?

See extract below from Codes of practice.

A2.7.1 Disclosure to second and third parties is limited to the following:

A2.7.1.1 Agencies or individuals that hold statutory powers to investigate or prosecute criminal or civil offences.

A2.7.1.2 Third party disclosures in line with the Data Commissioners Code of Practice for CCTV and the Data Protection Act 2018

A2.7.1.3 People whose images have been recorded and retained (this is a subject access request under the Data Protection Act 2018). Images will not be disclosed in instances where disclosure to the individual would prejudice criminal enquiries or criminal proceedings, or in instances where an individual has been unable or unwilling to provide a time, place and date by which the data controller can conduct a data search. The data controller undertakes to search within one hour each way of the time supplied by the individual. In any instance where the individual making the request is unknown to the data controller then it is a requirement that the individual provides a suitable photograph of himself/herself so that an accurate identification of the individual can be made within the recorded data.). All subject access requests should be referred to the Council's Information Governance Team for centralised logging and monitoring of responses. A charge of £10 will be made for each application for disclosure under this clause

A2.7.1.4 All requests for disclosure and any subsequent refusal will be documented by the data controller; a record will be kept of any complaints and the decisions resulting from the said complaints.

A2.7.1.5 All data subject access requests will be referred to the Information Governance Team who will process the request and input onto the Council's FOI System ensuring that all necessary information is obtained.

A2.7.1.6 The Information Governance Team will designate a responsible manager to deal with each application for disclosure. All staff to whom an application may be sent to

will be able to recognise the application and be able to pass the application to the designated responsible manager.

A2.7.1.7 In dealing with the application for disclosure the designated manager will consider prior to any disclosure whether the images of third parties are held under a duty of confidence. (First and Sixth Data Protection Principle) In this instance the identities of other individuals whose identifying features appear within the recorded data will have their images blurred so as to protect their identity where required. The data controller can make a charge should this editing be required. Details of these costs will be notified to the applicant once the data controller has completed a successful data search.

A2.7.1.8 Any applicant refused disclosure will receive a written response within 40 calendar days in which the Information Governance Team will set out the reasons why a disclosure request will not be complied with.

A2.7.1.9 Where it is decided that the publics' assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident, recorded CCTV images may be disclosed to the media. Images will only be disclosed to the media after receipt of legal advice. As part of that decision, the wishes of the victim of an incident will be taken into account. In all cases of media disclosures for the purposes of this clause the police authority will have the sole discretion of disclosure.

37. Do you have a written policy on the disclosure of information to any third party? ☒ Yes ☐ No

38. How do your procedures for disclosure of information guard against cyber security risks?

Any FOI subject access requests are encrypted by the Information Governance Team and a password provided.

39. What are your procedures for Subject Access Requests where a data subject asks for copies of any images in which they appear?

See 36 and links below.

https://www.southtyneside.gov.uk/article/35109/Disclosure-of-CCTV-images.

https://www.southtyneside.gov.uk/article/35108/CCTV-and-data-protection.

40. Do your procedures include publication of information about how to make a Subject Access Request, and include privacy masking capability in the event that any third party is recognisable in the images which are released to your data subject?

☒ Yes ☐ No

41. What procedures do you have to document decisions about the sharing of information with a third party and what checks do you have in place to ensure that the disclosure policy is followed?

All requests are administered by the information team and a specific system and all decision logged and audited.

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

☒ Yes ☐ No

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.

(There are lists of relevant standards on the Surveillance Camera Commissioner's website: https://www.gov.uk/guidance/recommended-standards-for-the-cctv-industry)

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

Surveillance Camera Commisioner Certification.

44. How do you ensure that these standards are met from the moment of commissioning your system and maintained appropriately?

On Site audit and annual desk top review.

45. Have you gained independent third-party certification against the approved standards? ☒ Yes ☐ No

46. Have you identified any areas where action is required to conform more fully with the requirements of Principle 8? ☐ Yes ☒ No

Action Plan

Principle 9

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

47. What security safeguards exist to ensure the integrity of images and information?

The Corporate ICT Network is PSN Compliant and all CCTV equipment behind firewalss. Regular audits carried out by ICT to identify vulnerabilities and recify through patches etc.

48. If the system is connected across an organisational network or intranet, do sufficient controls and safeguards exist? ☒ Yes ☐ No

49. How do your security systems guard against cyber security threats?

See 47.

50. What documented procedures, instructions and/or guidelines are in place regarding the storage, use and access of surveillance camera system images and information?

See codes of practice at Link below.

https://www.southtyneside.gov.uk/article/35108/CCTV-and-data-protection.

51. In the event of a drone mounted camera being lost from sight, what capability does the pilot have to reformat the memory storage or protect against cyber attack by remote activation?

N/A

52. In the event of a body worn camera being lost or stolen, what capability exists to ensure data cannot be viewed or exported by unauthorised persons?

None at present.

53. In reviewing your responses to Principle 9, have you identified any areas where action is required to conform more fully with the requirements? If so, please list them below.

☐ Yes ☒ No

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.

54. How do you review your system to ensure it remains necessary and proportionate in meeting its stated purpose?

Through Surveillance Camera Commisioner Ceritfication Audit and annual desk top review.

55. Have you identified any camera locations or integrated surveillance technologies that do not remain justified in meeting the stated purpose(s)? ☐ Yes ☒ No

56. Have you conducted an evaluation in order to compare alternative interventions to surveillance cameras? (If so please provide brief details) ☒ Yes ☐ No

This happens as part of various meeting such as ASB Taksing and Safer Neighbourhood Meetings. All options and considerations are documented and a proportionate response is decided..

57. How do your system maintenance arrangements ensure that it remains effective in meeting its stated purpose?

Two annual maintenance visits a year carried out by a SSAIB Certified Company.

58. Have you identified any areas where action is required to conform more fully with the requirements of Principle 10? ☐ Yes ☒ No

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.

59. Are the images and information produced by your system of a suitable quality to meet requirements for use as evidence? ☒ Yes ☐ No

60. 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 requirements for evidential purposes?

Police and Anti-social Behaviour Unit, Council Legal dept.

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

62. Is the information in a format that is easily exportable? ☒ Yes ☐ No

63. Does the storage ensure the integrity and quality of the original recording and of the meta-data? ☒ Yes ☐ No

64. Have you identified any areas where action is required to conform more fully with the requirements of Principle 11? ☐ Yes ☒ No

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.

65. What use do you make of integrated surveillance technology such as automatic number plate recognition or automatic facial recognition software?

None

66. How do you decide when and whether a vehicle or individual should be included in a reference database?

N/A

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

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

N/A

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

70. Have you identified any areas where action is required to conform more fully with the requirements of Principle 12? ☐ Yes ☒ No

Action Plan