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.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	Plymouth City Council
Scope of surveillance camera system	401 CCTV Cameras 11 ANPR Cameras for Bus lane enforcement 43 Handheld ANPR cameras for Parking enforcement 30 Body worn cameras
Senior Responsible Officer	Darren Stoneman
Position within organisation	Civil Enforcement Manager
Signature	
Date of sign off	16/03/2020

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 following are objectives of Plymouth City Council CCTV Scheme and have been published in the Plymouth City Council CCTV Operations Policy 2020

A copy of which is available to the public on our website

• Deterring crime and assist in the detection of criminal offences

• Deterring anti-social behaviour and assist in the detection of anti-social behaviour incidents

• Reducing the fear of crime and anti-social behaviour

• Improving the safety and security of residents, visitors and the business community

who use the facilities covered by the CCTV scheme.

• Assisting the emergency services in the location of Missing Vulnerable persons.

• Traffic Enforcement under the legislation below:-

The Road Traffic Act 1988

The Traffic Management Act 2004

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

The introduction of the Section 7 of the Crime and Disorder Act 1998 placed a direct responsibility on local authorities to combat crime and anti-social behaviour. This provides a statutory framework enabling local authorities to consider how their services could contribute to reducing crime and disorder, as well as their impact on social and community factors against that affect crime levels. The Council's CCTV Service supports Plymouth City Councils corporate priorities to make the City Safe, Caring, Healthy, Vibrant, Thriving, Green and Attractive for residents, Visitors and businesses alike. DPA 2018, Part 3 – Allows Plymouth City Council to act as a competent authority and process personal data including Special Category Information for the prevention, investigation, detection or prosecution of criminal offences.

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

A Public Space CCTV system that is maintained and operated to a high standard is a proven tool in detecting crime, and the perpetrators of it. CCTV is used to enhance public safety and can reduce the time and cost on law enforcement services investigating allegations of crime by providing high quality Primary and Secondary evidence for all that require it.

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

None

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?

no, an assessment has been considered and updated and published on our website

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

☐ Yes ☒ No

Action Plan

biometric and recognition software is not used

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?

Plymouth City Council has a corporate complaints policy. The maximum amount of time given for responding to a stage one complaint is 10 working days. If the complaint cannot beresolved on the spot, then the service must acknowledge the complaint within five working days and resolve to deal with the complaint in the remaining time left.

The full complaints policy and procedure can be found of the Councils Website here:

https://www.plymouth.gov.uk/selfservice/feedbackandcomplaints/makegeneralcomplaintcomplimentorgiveusyourfeedback

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

Action Plan

The Council is in the process of upgrading its entire CCTV Public Space CCTV Network We will be observing the provisions of the Passport to Compliance and will be undertaking a Public Consultation regarding the use of CCTV within the city in late 2020

Body Worn CCTV is incuded within this review, however a separate policy is in place

https://www.plymouth.gov.uk/sites/default/files/Body-Worn_CCTVPolicy.pdf

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?

The Public Space CCTV system is currently managed within the Place Directoratet. The Cheir Executive Officer has been nominated as the Single Responsible Officer (SRO) and as such is responsible for its lawful operation. The Single Point of Contact for Plymouth City Council CCTV systems in the CCTV Manager, who reports to the Parking, CCTV & Marine Group Manager, who in turn reports to the Head of Highways . A full Organisation chart can be found in the CCTV Operations Policy.

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

This included within the CCTV policy outline done our Website and is the Civil Enforcement Manager. The counciols data policy can be found

https://www.plymouth.gov.uk/aboutcouncil/accessinformation

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?

All staff members with responsibility for operating the CCTV system follow the processes and procedures stipulated in the Control Room Operations Manual ensuring that best working practice and responsibilities are defined and auditable.

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

CCTV system is wholly owned by Plymouth City Council

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?

All PCC staff operating the CCTV system are qualified to BTEC level 2. The Council also operates an appraisal system which comprises of one to one meetings with staff and their line manager where competency and training issues can be discussed and training can be arranged where required. Workshop training sessions arranged with staff to enable best practice working to be communicated

The staff contractor Enigma Security Solutions undertake SIA and compliance training with all staff

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?

All staff have attended SIA training and new contract for CCTV staffing focusses on development of staff and regular training

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?

All operators are Police and SIA certified,
PCC employees (Manager are trained but not certified)

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?

Yes, please see content of BWV POlicy https://www.plymouth.gov.uk/sites/default/files/Body-Worn_CCTVPolicy.pdf

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

Not Applicable

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

☐ Yes ☒ No

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.

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?

Images are stored for 28 days to assist the Police and other law enforcement agencies in the apprehension and prosecution of those committing crime and public disorder. If footage is requested by Investigating Officer the Council have the ability to store these images for an additional 7 days to allow for collection. After 35 Days from initial recording images will be deleted unconditionally. We feel these retention periods allow for the gathering evidence by a fair and accountable method.

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

The VMS automatically erases video footage 28 days from the date of original recording.

The CCTV Manager is responsible for the deletion of footage from the evidence locker once it is time expired.

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?

Access is agreed by the Senior Responsible Officer, Community Safety manager and the CCTV Manager. Access is limited to those with a statutory responsibility to investigate Anti-Social Behaviour, Crime and Council Regulatory services such as Trading Standards, Environmental Enforcement, Neighbourhood Safety and Food Safety. Footage will never be released for entertainment purposes.

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?

Disclosure is normally by means of DVD disc, Encrypted USB Memory Stick or Encrypted

Portable Hard Disk Drive. The use of email is not permitted or is any other electric data transfer i.e. Dropbox

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

a) Data Subject Contacts Council within 31 days with details of footage they require.

b) Search carried out

c) Data Subject notified of outcome of search

d) If positive search, footage reviewed by CCTV Manager with regard to blanking

faces of other subjects that can identified in footage.

e) Footage exported to appropriate media.

f) Data Subject Identity checked.

g) Footage disclosed.

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?

Plymouth City Council has a written and auditable procedures to cover disclosure to law enforcement agencies, solicitors & insurance companies and subject access requests. We do not disclose to the media and this is documented in the Councils Public Space CCTV Operations policy. The CCTV Manager carries out random audits of all disclosures.

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?

BS EN 62676-1-1 – Video surveillance systems for use in security applications

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

The installed CCTV system will be tested and maintained in accordance with

BSEN62676-4. The council has an inhouse CCTV engineer to undertake this work. The engineer has industry leading qualifications in design, maintenance and delivery

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

CCTV engineer to produce maintenance schedule

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?

All CCTV footage is stored on encrypted or password protected hard drives. The VMS system keeps an extensive audit log of the processing of video footage stored as part of its systems. Manual and electronic systems are in place to be able to audit the Rapid Deployment and Mobile Cameras; as although their footage is protected in a similar way to the Public Space footage these system do not provide anautomatic audit trail

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?

All key systems are protected by Password or PIN. Unused network connection ports are locked down. Network switches and other transmission utilise MAC Address locking to prevent unauthorised equipment being connected to the network

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

Procedures for the management of recorded material are documented in the CCTV Control Room Procedural Manual.

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?

Not Applicable

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?

The Audax system is passwoord protected and can only be downloaed to proprietry software with the correct access

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?

Reviews of the CCTV system are carried out annually. Crime Maps are produced and camera locations are compared to the maps. Public consultation will be undertaken in the form of a survey.

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

we currently feel that the security provided to residents of having CCTV cannot be replicated with additional police of PARC rangers at the current time and lihting and street design alone do not provide the assurance required.

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

The Council has an inhouse maintenance engineer with a specialist skill set in the CCTV network in Plymouth. Two Pre-Planned maintenance visits are carried out annually, response repairs on a priority scale are also undertaken. The is 24/7 support in case of emergency which is currently

defined as:-

• Any fault causing an immediate Health & Safety Risk.

• Loss of power or control

• Loss of VMS

• Loss of Video or Control of more than 5 cameras

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

Action Plan

further scope for replacement programme needed from CCTV engineer

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?

Full complaince with the requirements from Devon & Cornwall Police CCTV officer was achieved, thus giving reassurance over system standard.

CCTV consultant was used to seek requirements across the city

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

not applicable

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?

ANPR is used to support the enforcement of parking contraventions in accordance with the Road Traffic Act and Traffic Management Act.

These cameras provide footage or stills to highlight the contravention for use in evidence

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

When a vehcile is deemed in contravention of a Valid Traffic Regulation Order in accordance with the legislation outlined above

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?

The document retention policy states that all parking data should be archived 6 years after the case closure date.

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

None