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	Blackpool Council
Scope of surveillance camera system	• Public Space CCTV; and • Use of Body Worn Cameras within the Public Protection Service (including Civil Enforcement Officers)
Senior Responsible Officer	John Blackledge
Position within organisation	Director of Community and Environmental Services
Signature	
Date of sign off	22nd June 2023

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?

Public Space CCTV (which is predominantly in the Town Centre) is deployed for the purposes of the prevention and/or detection of crime and to combat anti-social behaviour.

The purpose of the deployment of Body Worn Cameras within the Public Protection Service (including Civil Enforcement Officers) is to safeguard employees and members of the public, in addition to providing evidence for all parties in the event of an investigation into an incident, accident or alleged crime.

A statement of need is included on the Council's website and contains the objectives of processing.

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

Blackpool Council primarily processes personal data from its public space CCTV network under the UK General Data Protection Regulation (GDPR), Article 6(1)(e) public task.

This basis is underpinned by Section 7 of the Crime and Disorder Act 1998 which places a direct responsibility on Council's to combat crime and anti-social behaviour. Section 163 of the Criminal Justice and Public Order Act 1994 empowers Council's to provide CCTV.

In relation to Body Worn Cameras This basis is underpinned by the Health and Safety Act 1974 which requires the Council to protect persons at work against risks to health or safety arising out of or in connection with activities at work.

There is also a raft of legislation supporting the enforcement action being taken which includes but is not limited to:

Antisocial Behaviour, Crime and Policing Act 2014, Consumer Credit Acts 1974 and 2006, Consumer Protection Act 1987, Consumer Protection from Unfair Trading Regulations 2008, Criminal Justice Acts 1988 and 1991, Criminal Justice and Police Act 2001, Environmental Protection Act 1990, Food Safety Act 1990, Food Safety and Hygiene (England) Regulations 2013, Health and Safety at Work etc Act 1974, Housing Acts 1985 (as amended), 1996, 1998 and 2004, Pollution Prevention and Control Act 1999

The Data Protection Act 2018, Part 3 allows Blackpool Council to act as a competent authority (where it has the powers to do so) to process personal data (including special category data) for the prevention, detection or prosecution of criminal offences.

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

A Public Space CCTV system acts as deterrent to crime and anti-social behaviour occurring in the first instance. This is because when maintained and operated to a high standard it is a proven tool in the detection and identification of perpetrators. CCTV is used to tackle common crimes within Blackpool including vehicle crime and shoplifting; the deployment of an effective system improves the general security of the main retail and leisure areas; both in terms of individual personal security and the security of premises and contents. As a popular tourist resort and also a deprived borough by national standards, the town centre is a particular location that suffers high numbers of incidents of crime and anti-social behaviour. This can cause residents and visitors considerable concern. Anti-social behaviour can include flyposting, begging, illegal street trading, vandalism and drunken behaviour. A high quality CCTV system can also reduce the time and cost on law enforcement investigating allegations of crime by providing high quality evidence, this increases the likelihood of the prosecution of offenders and justice for the individuals concerned.

Deployment of body worn cameras is to safeguard staff and members of the public and to provide evidence for all parties in the event of any investigation into incidents, accidents or alleged assaults. Given the nature of the roles within the Public Protection Service such as Civil Enforcement Officers, its employees are at particular risk of verbal or physical abuse. The Public Protection Service is responsible for enforcement against a raft of legislation and evidence gathered from Body Worn Cameras is important in terms of executing its powers effectively and obtaining successful prosecutions.

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

Development of procedures for the use of Body Worn Cameras within the Public Protection Service has taken place as part of this review of documentation.

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?

Not applicable.

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

☒ Yes ☐ No

Action Plan

Apply fixed review dates to the two CCTV related Data Protection Impact Assessments (DPIAs) covered by this assessment.

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?

Under the Data Protection Policy and Personal Data Breach Procedure the Council's statutory Data Protection Officer is responsible for the investigation of any complaints in relation this type of processing (as it relates to the processing of personal data). This and their contact details are included within the Council's published privacy information.

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

Action Plan

Council's published corporate privacy notice is to be reviewed as part of this review of documentation.

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 Council has in place a Corporate Working Group with responsibility and oversight of the use of CCTV; members of said group include:

Director of Governance & Partnerships (Chair), Director of Community & Environmental Services, Head of Public Protection, Head of Legal Services, Senior Responsible Officer (SRO), Head of Audit & Risk, Data Protection Officer (DPO).

Robust suite of a policies and procedures are in place, includes Data Protection Policy, CCTV Code of Practice, Body Camera Procedure, Personal Data Breach Procedure.

Internal audit programme includes CCTV has one of its work streams.

Data Protection Officer (DPO) conducts regular reviews of key documentation such as Record of Processing Activities (RoPA), privacy information, data protection impact assessments etc.

Training programme includes numerous strands with all employees undertaking data protection training, selected staff involved in the use and governance of CCTV undertaking specialist training.

Employees undertaking CCTV monitoring hold SIA licenses and all employees have confidentiality as part of their contract. .

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

Data Protection Officer (DPO) whose details are included in all privacy information acts as the SPOC.

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?

The Council has in place a Corporate Working Group with responsibility and oversight of the use of CCTV; members of said group include:

Director of Governance & Partnerships (Chair), Director of Community & Environmental Services, Head of Public Protection, Head of Legal Services, Senior Responsible Officer (SRO), Head of Audit & Risk, Data Protection Officer (DPO).

Robust suite of a policies and procedures are in place, includes Data Protection Policy, CCTV Code of Practice, Body Camera Procedure, Personal Data Breach Procedure.

Internal audit programme includes CCTV has one of its work streams.

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

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?

The Council has robust supervision, line management and appraisal processes in place; these assess employees compliance with the above and identify any areas for improvement. The Council ensures operatives of CCTV hold SIA licenses and there is robust induction, training and mentoring measures in place.

The Council has in place a Corporate Working Group with responsibility and oversight of the use of CCTV.

Internal audit programme includes CCTV has one of its work streams and this provides independent assurance.

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?

Not applicable.

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, contained within a Body Worn Camera Procedure.

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 as technology not used.

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

Action Plan

Consider occupational standards for CCTV.

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?

One month (31 days) which is based on industry best practise and two years if required for investigatory purposes.

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

Automatic deletion applied.

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

Consider whether an periodic interim review can take place where footage is retained for two years for investigatory purposes.

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?

Role based permissions with a strict authorisation procedure in place for persons within specified roles. These roles are then reviewed as part of the data protection impact assessment process and within internal audits.

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 made via the NICE Digital Evidence Management Solution which has been subject to a data protection impact assessment and due diligence. In the event of the former not being a viable option a password/encrypted protected disk is made which is obviously not vulnerable to cyber-attack as its offline.

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

Specific Right of Access Procedure in place for the Information Governance Team to process said requests and this procedure is communicated to members of the public on the Council's website. The Council also has pixilation software to assist with third party redactions.

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?

Procedure is managed centrally by the Information Governance team and a disclosure log is maintained documenting decision making.

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?

The data is housed on the Council's ICT infrastructure which holds Public Services Network (PSN) and Cyber Essentials Plus accreditation/standards. CCTV operatives hold SIA licences.

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

The Council has a place a Data Protection Impact Assessment Procedure and adopts a 'privacy by design' culture to ensure required standards are met prior to any system that processes personal data being procured. The GDPR Procurement Procedure contains controls to ensure this cannot incur without the necessary assessments.

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 data is housed on the Council's ICT infrastructure which holds Public Services Network (PSN) and Cyber Essentials Plus accreditation which provides technical assurance. External penetration testing also occurs and all devices are encrypted.

All staff are undergo a thorough induction, mentoring and training programme; with operatives holding SIA licenses.

Confidentiality clauses are also contained within contracts and internal audits provide independent assurance of compliance.

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?

The data is housed on the Council's ICT infrastructure which holds Public Services Network (PSN) and Cyber Essentials Plus accreditation which provides technical assurance. External penetration testing also occurs and all devices are encrypted.

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

Boddy Worn Camera Procedure, CCTV Code of Practice, Data Protection Policy, ICT Security and AUP, Right of Access Procedure.

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?

Devices are encrypted.

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?

Data Protection Impact Assessments (DPIA's) are reviewed regularly and an assessment is required for any new processing activity or a change to existing one.

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

Alternative measures considered as part of the Data Protection Impact Assessment, such as increased patrols of Police/Bid Wardens and/or better lighting. However, it was determined these alternative measures still require to be supported by use of CCTV to achieve its objectives.

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

Robust contractual clauses ensures system is maintained to an effective standard.

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?

Consultation took place with a number of stakeholders when the Council procured a new system, these included the Police and Blackpool Business Improvement District (BID).

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?

No automatic facial recognition undertaken and the Council' only use of ANPR is for car parking purposes (entry and exit).

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

Not applicable as not undertaken.

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?

Not applicable

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