

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	Breaston Parish Council
Scope of surveillance camera system	The current CCTV system comprising of 4 cameras was installed in Duffield Close in 2016 as an upgrade to the previous system which was installed circa 2000. The Parish Council had experienced high levels of Anti Social Behaviour around the Green, Blind Lane and on the Memorial and Sensory Gardens (drug taking, alcohol consumption, Anti-Social Behaviour). The police and safer neighbourhoods team supported the installation and positioning of the cameras. The cameras contribute to a reduction in alcohol / drug related disorder and ASB and improve public perceptions of personal safety for users of Duffield Close and the related gardens and their general feeling of safety whilst visiting businesses in the Green.
Senior Responsible Officer	Nicala O'Leary
Position within organisation	Clerk / RFO

Signature

--

Date of sign off

04/05/2021

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 current CCTV system comprising of 4 cameras was installed in Duffield Close in 2000 as a community initiative with the Scout Hall and the Parish Council. High levels of Anti Social Behaviour around the Green and Duffield Close (drug taking, alcohol consumption, anti-social behaviour). Issues were raised by the Scout Group and local businesses. The police and safer neighbourhoods team supported the installation and positioning of the cameras. The cameras help to reduce ASB by acting as a deterrent to disorder, and recording evidence when it does occur, they also improve public perceptions of personal safety for users of Duffield Close and people visiting businesses in the Green.

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

Under section 17 of the Crime and Disorder Act 1988 a local council has a duty 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,

- crime and disorder in its area (including anti social behaviour and other behaviour adversely affecting the local environment
- the misuses of drugs, alcohol and other substances in its area and;
- re-offending in its area

In addition Section 31 of the Local Government and Rating Act 1997 permits a local council, in order to prevent or detect crime to:

- install and maintain any equipment
- establish and maintain any scheme, or
- assist others to install and maintain any equipment or to establish and maintain any scheme

The Law Enforcement Directive (LED) enables the Council to process personal information without some of the normal safeguards required by the General Data Protection Regulations. LED controls the processing of personal data where it relates to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of threats to public security. The Council also uses CCTV camera systems under Section 163 Criminal Justice and Public Order Act 1994.

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

The system is necessary to prevent crime and disorder within the Green area and Duffield Close and is necessary to assist the relevant approved authorities with evidence for crime

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?

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

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?

Concerns or complaints can be made by contacting Breaston Parish Council and following the complaints procedure
https://www.breastonparish.co.uk/Complaints%20Procedure_Feb_2015.pdf

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?

We have a CCTV policy and procedure, only the clerk, caretaker & Chairman can access the system to view the recorded images and download as appropriate

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>

The Senior Responsible Officer contact information is listed within the CCTV policy and procedure

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?

Regular review of the policy and procedures and we also have an internal auditor who performs an annual review. All requests for the system to be reviewed are logged and identification of the requestee is always checked prior to any data being given via a memory stick

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?

We employ an external CCTV supplier on a maintenance contract to ensure that the system has regular updates and provides training as required. The CCTV policy and procedures are reviewed and approved by full council once a year / upon any changes to Data Protection / GDPR / relevant laws

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?

Training via the CCTV supplier for the operation of the system. Knowledge training via ICO / Surveillance Camera Commissioner guidance

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?

Not applicable

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?

The maximum period for storing images from the cameras is 14 days. The NVR is on a continuous loop and records over the previous data. If we are asked to supply images / footage within the 14 day period for the evidence of a crime, we supply this on a memory stick in person to the requestor, if an individual requests their personal data, we supply this via a memory stick in person to the requestor. In both instances, the person requesting the data is required to provide proof of their identity

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

Automatic loop system of a 14 day period, the images are automatically deleted.

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?

The Parish Council resolved that access would be restricted to the Clerk (as the Proper Officer of the Council) and to appoint the Clerk as the Senior Responsible Officer for the CCTV system plus the Caretaker to cover for the Clerk when on leave / not working for any other reason, with the Chairman as an emergency cover also.

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?

Information will only be disclosed when requested by an approved, authorised authority such as the police.

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

Individuals will be asked to provide a photograph of themselves so that the operator can recognise them on the recording and an estimate of the time(s) they were at the Leisure Green over the past 14 days (or the time they are requesting to be reviewed) All requests are subject to operational considerations for example where; - Footage has been requested by and/or passed to the Police as part of an investigation of a crime; or - Footage has been requested in respect of a road traffic collision and the information has been passed to insurers; or - Any relevant exemptions that might be considered to apply in respect of the Data Protection Act 1998.

- A complaints procedure that can be used for any complaints received regarding CCTV operations. Anyone wishing to make comments or observations about the CCTV system should write or email the Clerk whose contact details can be found in the CCTV Policy.

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?

CCTV log and policy

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 system is installed to the current standards, we are registered with the ICO and we have adequate signage in place. We have purchased a maintenance contract for the system to ensure that the software is regularly updated and that we have an adequate call out for system failures or faults with the cameras

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

The maintenance contract

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 NVR is situated in a locked cupboard within the Clerk's office which is locked and within the Parish Meeting Rooms which are also secured by two locked outer doors. The NVR is password protected. The key to the cupboard is kept in a locked safe which operates on a pin number.

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?

It is a stand-alone system with very low risk of cyber security. The data is only downloaded to a memory stick upon approved requests and handed over to the approver in person

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

CCTV policy and 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?

Not applicable

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?

Annual maintenance contract for software updates and system reviews. Changes would be made if new guidance / laws were introduced. The policy and procedures are reviewed on an annual basis by the Council or sooner if laws or new guidance were introduced.

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

Duffield Close is a public open space but also a public right of way so cannot be closed at night to prevent young people gathering in the gardens etc. The provision of CCTV was seen to be the only way forward when it was first installed.

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

Yes - we have a contract in place to cover any outages or damage to the system or 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

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?
- Approved by the Senior Responsible Officer as per the Surveillance Camera Commissioner Buyers Toolkit
-
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?

Not applicable

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

Not applicable

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?

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