

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	Norfolk and Suffolk Joint Custody
Scope of surveillance camera system	Norfolk and Suffolk Custody command operates a CCTV system in and covering the external premises at all 6 designated custody suites known as Police Investigation Centres (PICs). The purpose of this self-assessment is to ensure when operating the custody CCTV system, it used in compliance with the Surveillance Camera Code of Practice.
Senior Responsible Officer	Chief Inspector Rob Wicks
Position within organisation	Head of Custody
Signature	
Date of sign off	

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?

CCTV is operated by Norfolk and Suffolk Custody command at its PICs and is used to assist in the management of persons who are detained for various reasons as well as voluntary attenders, and to provide a safe working environment for detainees, voluntary attenders, staff and visitors.

Within each of the PICs there are a number of fixed position and some PTZ (pan, tilt, zoom) cameras that have the ability to capture visual recordings in high definition. In the charge areas inside the PICs there are also microphones to capture audio, which is recorded on the same system as the CCTV. CCTV cameras are located throughout each PIC including the van dock and entrance areas, holding areas, charge desk, corridors, cells and consultation rooms. These are not public places. However there are also CCTV cameras which cover police premises outside the PIC which are accessible to the public as well as secure external areas.

The use of the custody CCTV system shall be for the purpose of:

- a. Improving the safety and security of detainees, staff and visitors to custody,
- b. Monitoring the welfare of all detainees held in custody,
- c. Reduce the incidence of self-harm particularly from detainees who have been assessed as high risk.

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

The processing will be under the Law Enforcement Directive within Part 3 of the DPA 2018. Norfolk Constabulary and Suffolk Constabulary are both competent authorities under the relevant legislation and each has a duty to deter and detect crime. They also have an obligation to gather evidence under the Police & Criminal Evidence Act 1984 and then retain and disclose such material under the Criminal Procedure and Investigation Act 1996. Equally, the processing is necessary in the public interest in order to maintain good order and discipline within the Police Service. Any CCTV footage that is downloaded will be kept in accordance with Norfolk and Suffolk Joint Force Policies and the NPCC retention schedule.

Norfolk and Suffolk Custody Command CCTV system is operated in line with Custody Standing Order 1.33 PIC CCTV which details the use of the CCTV system. It is also supported by Norfolk and Suffolk Joint Force Policy Information Management and associated policies that provides guidance on information management underpinning the legal and national guidance and standards relating to information management.

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

The prevention, detection and investigation of crime and complaints and internal conduct matters. CCTV is constantly recorded and not selectively operated to record any specific individual, group or time. The custody CCTV system is an essential tool to support the legitimate aim of maintaining the welfare and security of people who are detained, work in or visit one of Norfolk and Suffolk's PICs.

The availability and use of custody CCTV is supported by the Independent Office for Police Conduct (IOPC), which examine deaths and serious incidents in police custody and recommended:

"Police forces should ensure that CCTV is available in at least one cell in the custody suite, to be used when a detainee is identified as being at risk, and, where available, that it is fully operational. Independent custody visitors should check that CCTV is operational when carrying out their custody visits."

4. Is the system being used for any other purpose other than those specified? If so please explain.

☐

Yes

☒

No

N/A

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

Action Plan

N/A

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?

N/A

6. Have you identified any areas where action is required to conform more fully with the requirements of Principle 2? ☐ Yes ☒ No

Action Plan

N/A

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?

Any concerns or complaints about the use of CCTV within custody, will be directed in the first instance to the custody sergeant, on duty at the relevant custody suite. The PIC Inspector will also be notified of any public 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

Locations of CCTV warning signs outside all 6 PICs have been reviewed by each PIC Manager and deemed to be in the best possible locations to notify those who may be within sight of the cameras that this is the case.

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 use of custody CCTV is overseen by Norfolk and Suffolk Custody Command and used in accordance with Custody Standing Order 1.33 PIC CCTV, which details the use of the CCTV.

It is also supported by Norfolk and Suffolk Joint Force Policy Information Management and associated policies that provide guidance on information management and underpin the legal and national guidance and standards relating to information management.

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?

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

The system is no jointly owned - it is owned and maintained on behalf of Norfolk and Suffolk Constabularies by a third party provider under the PFI contract.

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?

- a. Custody staff have been trained in the correct use of the custody CCTV system and that it is always to be used in compliance with Custody Standing Order 1.33 PIC CCTV.
- b. Access to the system is password protected, and the access or use of the custody CCTV system can be monitored via a CCTV management software program.
- c. Use of the system is restricted to authorised Norfolk and Suffolk Custody staff and for maintenance by the contractor only.

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?

N/A

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 users are trained in the use of the system and is used in accordance with Custody Standing Order 1.33 PIC CCTV.

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?

The use of body worn video is detailed on a separate privacy impact assessment.

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

N/A

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?

See section 2 below

Any CCTV footage required as evidence will be downloaded and saved in accordance with Custody Standing Order 1.33 PIC CCTV, which is supported by Norfolk and Suffolk Joint Force Policy Information Management and associated policies which provide guidance on information management and underpin the legal and national guidance and standards relating to information management.

Where the CCTV provides evidence of an offence it will be retained in accordance with the Management of Police Information guidance which sets timescales dependent upon the nature of the offence - 6 years for a MOPI 3 offence, 10 years for a MOPI 2 offence and 100 years for a MOPI 1 offence.

Individuals can make a Subject Access request to confirm what personal data is held by Norfolk or Suffolk Constabularies.

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

Non-evidential & if no complaint is anticipated the CCTV data will be overwritten to prevent unjustified retention. The custody CCTV system used within Force buildings can hold 60 days of 'live feed' which is stored on a local drive. After those 60 days, unless the stored CCTV has been saved as evidence, the previously recoded CCTV will be overwritten.

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

N/A

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 to custody CCTV is determined by the reason for retention. Images and audio required for evidential purposes, whether for criminal investigation or relating to complaints or conduct matters, are transferred to the Digital Asset Management System (DAMS) in relation to which there are separate policies regarding management of such assets. Access to those assets is restricted to the investigator and anyone they have a legitimate need to share it with, such as the Crown Prosecution Service, IOPC etc.

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?

Downloaded custody CCTV footage is kept on DAMS, for which the access is password protected.

Any disclosure of the downloaded custody CCTV i.e. evidence to be sent to the Crown Prosecution Service will be disclosed via secure means, to safeguard against cyber, data or information security risks.

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

Subject access requests are considered and managed by Norfolk and Suffolk Joint Information Management team.

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?

The custody CCTV is only accessible via a secure IT network, and will be accessed only by authorised police users.

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

☐

Yes

☒

No

Action Plan

N/A

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 and BS EN 62676-4 and also NSI/SSAIB standards for the installation and management of CCTV systems

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

These standards are maintained on a daily basis by a contractor who are an SSAIB approved installer and maintainer of CCTV systems and hold the ISO accreditations of 9001, 14001 and 27001

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

Consideration of third party certification against the approved standards, however this is a decision for the contractor as this was not part of the specification for the contract. It may be that when the contract comes up for renewal then the Constabularies may seek to include this in future contracts, which will be considered on its merits at the time.

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 following safeguards are in place to support the operation of the custody CCTV;

- a. The system operates on a secure IT network, which is protected against cyber security risks.
- b. Access to the CCTV system is limited to authorised personnel and is password protected to guard against unauthorised use.
- c. Images or CCTV footage that has been downloaded as evidence is kept securely in accordance with MoPI guidelines.
- d. The use of the custody CCTV system is also supported by Custody Standing Order 1.33 PIC CCTV and associated policies that provide guidance on information management which underpin the legal and national guidance and standards relating to information management.

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 custody CCTV system operates on a secure IT network that has enhanced security through appropriate levels of security protection.

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

The use of the custody CCTV system is used in accordance with Custody Standing Order 1.33 PIC CCTV and associated policies that provide guidance on information management which underpin the legal, and national guidance and standards relating to information management.

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?

N/A - this is covered under separate policies relating to body worn cameras.

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

N/A

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?

All Norfolk and Suffolk PICs are inspected annually, which includes the maintenance and testing of the custody CCTV system.

PICs are subject to regular external scrutiny and inspection by independent custody visitors following their visit they provide feedback about issues they have identified from their visit.

Any issues associated with the operation and use of the custody CCTV system will be raised with the Custody Command team.

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

N/A

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

The PIC CCTV system is supported by a PFI maintenance contract, which includes a fault reporting process where reported faults are repaired as soon as possible to ensure the custody CCTV operates as effectively as possible.

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

☒

Yes

☐

No

Action Plan

During the annual custody maintenance program, a site survey will be carried out to ensure the custody CCTV cameras are sited in the correct locations, and there remains a legitimate reason for the CCTV system to remain in place.

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?
- The custody CCTV is installed within a police setting and the use of the system requires the capability to be able to download images of evidential quality.

The technical and operational requirement for the system was set by Norfolk and Suffolk joint Custody Command prior to installation in order meet the appropriate user requirements.
-
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

N/A

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?

N/A

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?

Images or CCTV footage that has been downloaded as evidence is kept securely in accordance with MoPI guidelines.

Depending on the nature of the offence the CCTV is been requested for, under MoPI guidelines the downloaded CCTV will be stored for 2, 6, 10 or 100 years.

The use of the CCTV system is also supported by Custody Standing Order 1.33 PIC CCTV and associated policies that provide guidance on information management which underpin the legal and national guidance and standards relating to information management.

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

N/A