Self Assessment Tool

How well does your organisation comply with the 12 guiding principles of the Surveillance Camera Code of Practice? Complete this easy to use self assessment tool to find out if you do.

Using this tool

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

It is possible to be largely compliant with some principles and to fall short against others. As a result you will note that at the end of the questions against each principle there is a space to include an action plan. This is so you can put actions in place over the next year to improve your compliance to that principle. These boxes can also be used to make a note of what evidence you could produce if required to show your compliance to that principle.

The template contains a combination of open and closed questions. For the open questions, there is a limit on how much you can write within the template, so please feel free to include any additional notes as an annex to the document – there are additional blank pages at the end of the tool to help you to do so.

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

Is this tool for me?

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

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

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

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

What should I do next?

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

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

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

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

Name of organisation	Northamptonshire Police
Scope of surveillance camera system	BWVC (Bodyworn Video Cameras) Motorola VB400 and X100 attachment
Senior Responsible Officer	Chris Hillery
Position within organisation	Superintendent
Signature	
Date of sign off	27th September 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?

It remains true that interactions by police officers and police staff with the public when attending incidents carries a risk to members of the public, offenders, property and police staff.

When incidents occur, clear evidence is vital in supporting investigations and detecting crime. There is a requirement to provide best evidence of incidents involving a police response. Whilst officers and staff provide accurate written statements and records of incidents, visually recorded evidence (VRE) often proves critical in providing evidence of an incident - providing mitigation against complaints, or supporting breaches of legislation or Force policy. Bodyworn video can provide an open and transparent view of an incident which is disclosable.

VRE is recognised by HM Government, PCCs and the police as a vital tool in crimefighting; and an opportunity to be more transparent with our community - building trust and legitimacy. Bodyworn video is used primarily for prevention and detection of crime, and are ideally placed to capture a range of incidents as well as other offences that fall under Criminal or Common Law.

A statement of need, BWV Policy, privacy impact assessment and SOPs are all completed and are reviewable annually or when a change is proposed/made.

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

Footage will be utilised, as above, for prevention and detection of crime; as well as providing best evidence for ongoing police investigations.

Human Rights Act has been considered in relation to the use of BWV. There is also a consideration under RIPA - however as devices are overtly fitted to uniformed officers whilst undertaking their duties, then the cameras will not fall under the scope of RIPA legislation.

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

Footage obtained is primarily used by uniformed officers/staff whilst on patrol, where the public expect evidence to be of the highest quality. Data is retained at direction of MOPI guidance and Force Policy.

The cameras are overt, clear and obvious for all to see - including when recording is activated. They visually light up and have audible alerts when recording is

initiated/stopped. Cameras will be used for specific incidents as dictated by Force Policy, and are not to be used for directed surveillance on a person or community.

The necessity of the recording is to capture best evidence of offences taking place, scenes, and stop search interactions. The recordings with maximise the quality of evidence offered to the court to support prosecutions.

Evidence gathered will support public confidence by showing officers/staff as open, honest and accountable.

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

UPDATE:
Since the last self-assessment completed in 2021, Northamptonshire Police has implemented a new managed system via Motorola (VB400 and X100).

This is an off the shelf system and consists of around 750 cameras utilising the secure VideoManager system. Data is transferred, edited, retained and deleted within Nice Investigates system.

This action is now complete and the units and software is fully up and running.

Outcome: Completed.

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 - DPIA reviewed annually alongside this document.

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

☒ Yes ☐ No

Action Plan

UPDATE

Last DPIA was signed off by DCC Nickless on 12th Feb 2021.

The last DPIA had some queries around 3 high level risks, namely:

- Loss of footage through interference
- Loss of availability due to a network problem
- Loss of footage from a connection error to DEMS

These have each been addressed. Front end user permissions are restricted - only the recording officer has the ability to delete recorded footage. As the recording officer knows what has been captured, it is their responsibility to delete material relating to a case that is no longer relevant, or tagging it to an occurrence for saving. The exception to this is administrator level access. All deletions are recorded in system logs, accessible in a restricted view.

It is accepted the only element that would not apply is where an occurrence number is not added, footage auto-deletes at 30 days as per MoPI and SOPs. This is not interference - this is lack of user action, however.

With regards to network problems and DEMS - the original copy is stored on Video Manager with a copy made when importing into DEMS. Should an error occur in DEMS there is a backup on VideoManager. The connector does not send data back from DEMS to VideoManager, providing a level of protection for the original data source.

Outcome: Completed.

Principle 3

There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

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

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

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

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

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

All complaints are treated following relevant policies and procedures.

There are several options for complaints depending on reported route. This ranges from departmental supervision, OPFCC, PSD, CCU and the IOPC. A complaint investigation may lead to a range of outcomes - from NFA (No Further Action) to criminal proceedings.

Any request for footage is dealt with by the Force Information Unit.

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

Action Plan

UPDATE:
From last self-assessment: Nominated person (Data Protection Officer) available via a link on the public facing Force website. Link to directly email the nominated person. Can be found under "Your Data Rights".

Outcome: Completed.

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?

There are clear, reguarly reviewed and updated Force Policies and SOPs governing the use of devices, and retention of captured footage. This must be adhered to by all officers and staff. New officers receive training as part of their intake.

Officers should activate recording as they are deployed to an incident and then download/tag/secure as appropriate. Evidence required for court/investigation is stored securely and kept for the required time as governed by MOPI.

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

Nominated person (Data Protection Officer) available via a link on the public facing Force website. Link to directly email the nominated person. Can be found under "Your Data Rights".

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?

Clear communication to staff who use BWV recording equipment. Line managers dip sample footage, particularly Use of Force ones. Stop searches require activation of a bodyworn camera, and these are always reviewed by a supervisor.

Professional Standards aware of usage and policy relating to BWV. All evidential footage and process are documented on Niche / VideoManager or NICE Dems as per evidential chains. All persons using these systems are required to have completed the training for this system.

Core training covers new recruits around use of BWV.

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

N/A

Core training liaised with as part of review of self-assessment. SPOC within core training for consistency.

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?

Officers are trained on the system, usage and legalities around the use of bodyworn video.

Copies of both the SOP and Policy are available to all through the Force Policy Library.

Requests for said policies can be placed via the Force Information Unit.

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?

As above - this forms part of initial training which all officers using the equipment will receive.

We also have a number of BWV Champions in-force who provide support and expert guidance to users and operational staff.

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?

SOP and policy detail this requirement for everyone to be clear. These are regularly reviews and any changes are cascaded down via Force Orders and other means (e.g. ACPO Vlogs).

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?

Data will be retained in line with MoPI guidelines with footage involving court procedings up to six years. Non-evidential footage will not be retained and should be deleted upon upload, at 30 days or when there is no longer a policing purpose to retain.

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

All users to be provided with guidance and training from BWV Digital Champions and written material.

All new users receive a 3 hour training input prior to using BWV.

All sergeants will be trained and will be expected to conduct regular checks with the officers, of their footage, to ensure the correct procedure is adhered to in retaining or deleting footage. This is currently manual and not automated.

As detailed above, supervisors must review all bodyworn video of stop searches and should dip sample use of force via Qlik system randomly.

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

UPDATE:
Automated system to ensure effective retention and deletion of footage. The new system includes this feature to delete either on upload or at 30 days. All legacy data pre June 2019 back to January 2018 being reviewed by the new BWV Data Coordinator. All data after June 2019 to be back record converted onto the new managed system when fully integrated.

Significant amount of work completed around this. There is a Retention and Deletion Procedure in place to address this. Further work ongoing.

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?

All data stored by Northamptonshire Police falls under the Data Protection Act and as such officers and staff are frequently reminded of the need for a policing purpose before accessing the footage.

There is a reminder of this when accessing VideoManager.

Northamptonshire Police monitiors all computer systems so breaches of this policy can be established. Footage of a sensitive nature or firearms incidents are restricted and can be cloaked where required.

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?

Northamptonshire Police maintains a strong firewall and data storage is managed within ISO guidelines.

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

All maters of this nature are handled by the Legal / Profesional Standards unit.

Any application must complete a request to the Force Information Unit who review each request and whether access should be granted or not.

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?

As above data is managed by the Force Information Unit who ensure all checks and policies are adhered to.

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?

I have reviewed BS 8593: 2017 Code of practice for the deployment and use of BWV.

System selected complies with The Surveillance Camera Commissioner current list of reccommended standards.

Footage is captured using a secure, suitable device which is time and data stamped and locked from editing unless pixelation is necessary.

Officers are trained on storage/retention/deletion of footage to further ensure standards are met.

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

Ongoing review of policy and procedures in relation to the usage and storage of data.

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

N/A

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 footage will be time stamped stored on a secure system.

All footage will be downloaded automatically (upon being docked) from the BWV device at the end of each tour and the device secured.

Current policy prevents a user from removing multiple devices.

The device will be purged of any data immediately following download.

The data is now stored directly onto Cloud storage via the Forces internal network.

Data cannot be obtained without being docked - i.e. you cannot connect to a computer with a USB to access the data. This provides an excellent layer of protection and security.

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?

Data is retained on a secure Cloud server with sufficient firewalls in place as per the Force Policy. Access to systems is controlled and only appropriate/authorised persons can gain access to data which is continually monitored and audited.

This process is managed via movers/leavers policy and the granting/removal of access is managed via that process.

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

In line with the Force policy around bodyworn video, data is captured and stored in an appropriate manner.

It should only be accessed and viewed by persons who have a lawful and necessary reason to view it and any breach of this policy falls within a profesional standards matter.

Checks can be made to identify officers/staff who have unnecesarily viewed footage if required.

A reminder of this is for each entry / access to the VideoManager system.

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?

All BWV is now recorded onto an fully encrypted system/camera.

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

UPDATE:
Mechanism is via a dock - multi-pin - not readily available to the public if the device was physically lost. There are suitable compression references (H.264) in place which is a significantly varied file format between manufacturers, as well as AES encryption keys which are necessary to enable download.

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?

Ongoing review by the working group. Re-assessing the SOP and policy annually in line with any changes legally or within force to confirm the policy still complies and is fit for purpose. Meets every three months.

Looking to refresh number of trained BWV Champions to give greater access for officers on the frontline to obtain support.

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

The alternatives were to not use any cameras leaving the force and officers open to criticism and risk.

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

Ongoing maintainance programme in place and all defects reported by the user.

Near miss / H&S Form exists also.

Any defective units to be identified and immediately sent for repair or replacement.

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

Action Plan

N/A

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?

Ongoing awareness from CPS.

Officers and staff review and engagement of new devices, system developments and changes through the BWV steering group.

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?

BWV not integrated with facial recognition or other similar system.

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

An asseement by the BWV user as to the evidential value of the footage and those captured.

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?

Automatic weed dates on on Niche are in place for individuals.

There is no automatic link between BWV and reference databases that would be pertinent under Principle 12.

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