



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	Leicestershire Police
Scope of surveillance camera system	Public Order/Public Safety Evidence Gathering Team EGT (Video Cameras)
Senior Responsible Officer	Kerry Smith
Position within organisation	T/ACC and Senior Information Risk Owner
Signature	
Date of sign off	August 2022

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 Order/Public Safety Evidence Gathering Team(s) (EGT) Overt Video Cameras can be utilised in all aspects of Policing at Public Order and Public Safety Events and brings with it opportunities to offer an improved service to the public, better quality and more robust evidence in criminal cases. It can also work to make the Police ever more efficient through behaviour modification in the presence of EGT, victimless prosecutions, fewer assaults on Police Officers, Police Staff (including PCSOs) and partners and therefore a reduction in the use of force.

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

Leicestershire Police is committed to making the best use of its resources. A key area of our strategy is to transform service delivery by taking full advantage of new technology. EGT is an overt tool by which Police officers can capture better quality evidence at the scene of a disorder or incident or crime. This processing will be conducted under part 3 of the DPA 2018, for law enforcement purposes so that Leicestershire Police can further its statutory obligations.

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

The objectives for EGT is to support the Leicestershire Policing priorities by enhancing opportunities for capturing best evidence; reducing challenges to evidence in the court; assisting police officers; police staff and partners to control anti-social behaviour; providing an optical evidence solution that will free up front line resources by increasing early guilty pleas, reducing office case preparation and court time, improve sanction detections and speed up the criminal justice process. As this method of surveillance is less intrusive and open and transparent, therefore it does not interfere with the fundamental rights of the attendees (public)

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

Not at this time

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 as DPIA has been completed.

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

Action Plan

Ensure DPIA is in place for 2021 and updated annually thereafter.

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 complaint received by Leicestershire Police for use of EGT Operators will be dealt with as per the Leicestershire complaints procedure. All EGT Operators are issued with proforma notices to inform members of the public about their rights regarding being filmed and these are handed to persons as required. A copy of the proforma is contained within the Leicestershire Police Public Order Evidence Gathering Procedure.

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

Action Plan

Information leaflet / proforma will need to be updated to reflect current legislation.

This has now been done. Leaflets are at reprographics - 05/06/2022

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?

Regional policy and procedural documents are in place for the use of EGT's. These are held by Derbyshire Constabulary as they are responsible for training all regional EGT staff and refresh their training every 12 months. The EGT policy is regularly reviewed by its author PC Lee Madin, Derbyshire Police. In place for Leicester Police is 'Leicestershire Police - Public Order Evidence Garthing Procedure'

The adherence to and the effectiveness of this policy and associated procedure is monitored by the Public Order/Public Safety Strategic lead.

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 single point of contact / senior responsible officer for surveillance camera governance arrangements is Leicester Polices Director of Intelligence currently Detective Superintendent James Avery. Leicester Polices 'How we use surveillance cameras' webpage has details on the deployment of surveillance cameras and contact details of the single point of contact / senior responsible officer

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?

Policy and Procedure are in place to ensure EGT trained Officers are aware of the lines of responsibility. Authority for use of EGT's is documented within the Silver Command decision log pertaining to the Operational deployment, detailing the rationale for deployment.

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

Update to Q13 - APP is presently being used - Action is to review Leicestershire Policy and current deployment procedures to bring this up to date.

Document updated and in process of being forwarded to COT - 25/05/2022

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 EGT Operators are refreshed on an annual basis to maintain their qualification. The cameras and the supporting system are reviewed on a regular basis by the College of Policing (CoP) as a National program.

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?

Not Applicable

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?

EGT Operators are trained and refreshed on an annual basis to maintain their EG qualification

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?

All EGT Operators will have Body Worn Video (BWV)

Recording an Incident on BWV. The decision to record or not to record any incident remains with the user, although the decision to record must be justifiable, necessary and proportionate to the circumstances the user is faced with.

Leicestershire Police have mandated that certain incident types should be recorded, these

include stop and search and domestic violence incidents. Users still have the option not to record, however a robust rationale will be required to be documented.

-
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

Not at this time

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?

Video footage that is created is reviewed by either the Dedicated Football Officer (DFO) or the Senior Investigation Officer (SIO), Disclosure or Exhibits Officer within 31 days. During that time it is either viewed and destroyed as not relevant, viewed and an intel item created and footage destroyed or kept for evidence for court proceedings.

Any Evidential or unused footage, and/or any DVD produced will be retained in line with the Management of Police Information (MoPI).

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

As the DVD's produced by the EGT Operators are a physical item there is no automatic deletion process .

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

Not at this time

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?

Responsibility is given to Staff and Officers to only view what is necessary and relevant and for a lawful purpose. Access to the DVD's created is the same as any other exhibit, the member of Staff or Officer has to sign the exhibit label to state when they took possession of the exhibit and will document where and when they viewed the footage and for what lawful purpose. Access to the personal data collected in the footage is held in a secure area with access only being given to those Officers and Staff on a need to know basis, i.e. involved in compiling files in relation to identified Offences.

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?

The camera's, SD cards, DVD burners and computers used are all Police assets and therefore have the appropriate levels of security. The the Surveillance equipment is kept within a secure, locked location. Computers are protected by password and bitlocker code.

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

Any requests for images under the Data subject Access Rights will be sent to the Information Management / Data Protection Department for processing.

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?

Material will be shared with the CPS for prosecution purposes or with another law enforcement agencies to prevent and detect crime. Any other such request will be directed through to information management for appropriate assessment and disclosure on a case by case basis.

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

Yes

No

Action Plan

Not at this time

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 Video Cameras used by Leicestershire Police meet the specification set out by the Home Office in the 2012 Review of Police Public Order Evidence Gathering Cameras. They are the same Cameras used by all Regional Police Forces, Northamptonshire, Derbyshire, Nottinghamshire and Lincolnshire.

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

The EGT Cameras were purchased from a Home Office supplied list of approved Cameras. This specified the technical specification that was required to be met and in order for the supplier to meet the required standards. The cameras were bought 'off the shelf'. No maintenance contract was entered into. Any faults reported on the cameras are rectified by commercial canvassing and best price. Prior to each deployment the EGT will conduct a check of the camera to ensure it is Operationally deployable.

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

Not at this 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 Video Camera's themselves do not hold any footage it is recorded onto a SD Memory card which is then transferred to DVD disc upon completion of the operation on a non networked burner. The disks are then processed as exhibits and handed over. The discs are treated as physical exhibits so are not held in a system that is connected to the internet. The SD Cards are reformatted after each use to erase any information prior to being used again.

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 Force IT Infrastructure is secured in-line with national policing requirements, with an annual assessment conducted by the Police Digital Service, to assure this, with this process supplemented by an annual penetration test of our environment, alongside internal processes such as the use of vulnerability management software to routinely scan our environment and remediate any vulnerabilities identified. The Force also benefits from the protections afforded by Office 365 utilising a number of these tools to safeguard our environment, with safeguards in place to safeguard our on-premise environment such as perimeter safeguards, encryption, anti-virus/anti-malware tools etc. The Force have a close working relation with the National Management Centre, who provide a number of services to Forces – protective monitoring, cyber threat intelligence and remediation advice etc.

Robust security incident management processes are in place within the Force and documented within bespoke procedures (both Cyber and traditional security incidents). An escalation process is in place to ensure that notification occurs to the relevant stakeholders within a timely manner, and within the legislated timeframe.

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

Leicestershire Police. Public Order Evidence Gathering Procedure. The transfer of evidence between the Leicestershire Police and the CPS is controlled by the CPIA and other agreements between the two organisations. The discs will only be played or stored on Leicestershire Police Computers. Once evidence/footage is with the CPS they will become the controller and responsible for the processing and security of it.

51. In the event of a drone mounted camera being lost from sight, what capability does the pilot have to reformat the memory storage or protect against cyber attack by remote activation?

Not applicable

52. In the event of a body worn camera being lost or stolen, what capability exists to ensure data cannot be viewed or exported by unauthorised persons?

The Cameras only have footage in them when in the hands of the EGT Operator. Policy, operating procedure and training ensure that Cameras are never left unattended and that they are cleared of ALL data after each operation. In the highly unlikely event that a camera were to be lost or stolen the previous footage may be viewed on the camera playback and would be held on the current inserted SD Card. There is no current capability to remotely erase or lock the 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

Not at this time

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?

Bound by College of Policing (CoP) reviews, last held in 2012, and adhere to their Policy. Equipment checks are carried out on the Cameras prior to deployment. Maintenance is carried out when faults are reported by the EGT's. The mandated training days are used as an opportunity to ensure that all six (6) Leicestershire Police EGT Camera's are functionally checked and all ancillaries are in place and serviceable. There is no formal maintenance programme in place.

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

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

Regular review and feedback. Post Operational deployment debriefs. Annual CPD day. Annual refresher training.

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

Yes

No

Action Plan

Confirmation with College of Policing that all policies / procedures in place and up to date

As per APP as directed by College of Policing.

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 review of 2012 by the College of Policing's predecessor was based on CPS requirements for a system that would provide usable evidence in court. College of Police provides and review the guidance and there predecessor along with the CPS would have conducted stakeholder engagement

61. Do you have safeguards in place to ensure the forensic integrity of the images and information, including a complete audit trail? Yes No

62. Is the information in a format that is easily exportable? Yes No

63. Does the storage ensure the integrity and quality of the original recording and of the meta-data? Yes No

64. Have you identified any areas where action is required to conform more fully with the requirements of Principle 11? Yes No

Action Plan

Not at this time

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?

None

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?

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

Not at this time