SURVEILLANCE CAMERA COMMISSIONER

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	Body Worn Video
Senior Responsible Officer	Kerry Smith
Position within organisation	T/ACC and Force 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?

These aims and ojectives are written in the Force BWV Policy and this is reviewed on a yearly basis.

Body worn video is a vital tool to support operational policing. It is used to capture and enhance evidence by way of audio and visually recording live, spontaneous and dynamic incidents as well as supporting officers in their interaction with the public when taking original written notes or accounts, which could have been misinterpreted or disputed. Furthermore body worn video is used to support the criminal justice system through evidence-based prosecutions and improving its efficiency by enabling an increase in early guilty pleas, reduce incidents of disorder through its overt use and how this affects subject behaviour, increase public reassurance and transparency, reduction in complaints against the police and quicker resolutions, improved discipline and use of force, and allow for reflective learning and training opportunities.

Objectives are outlined through East Midlands Regional Body-Worn Video Procedure, Leicestershire Police Body Worn Video Policy and Leicestershire Police Body Worn Video Privacy Impact Assessment.

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

The lawful basis for the use of Body Worn Video is supported by the Government legislation and policy that the police work to. The Police use a various framework of legislation and guidance applications, including the General Data Protection Regulations (GDPR), the DPA, the Surveillance Camera Code, Management of Police Information 2005 (MoPI) made under the Police Act 1996 and Police Act 1997, Common Law and the Criminal Procedure and Investigations Act 1996 and Code of Practice issued under Part II of that Act (CPIA).

Compliance with the Data Protection Legislation (i.e. the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA)) Processing will be conducted under part 3 of the DPA 2018, for law enforcement purposes so that Leicestershire Police can further its statutory obligations and execute their duties to prevent and detect crime.

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

The BWV cameras are justified as necessary and proportionate and are deployed in the interests of national security, public safety, the prevention of crime and disorder and the protection of the health and safety of Police personell. They are used to collect evidence and in doing so help detect, deter and disrupt criminality at a local, force, regional and national level.

Body worn video is personal issue to all front line officers and is not set to permanently record; it is down to the individual officer to begin the recording using their judgement and discretion. If an officer activates their camera it should be for a legitimate aim, taking into account their lawful purpose, policy and procedure and training they have received.

Audio recording is more intrusive than just visual recording however this continues to be necessary and proportionate because it allows evidence to be captured in an indisputable fashion, and if the camera is dislodged and the lens is pointing away from the incident then the capture of audio will be important. The presence of audio will also increase levels of transparency and ensure context is provided to interactions.

Use of body worn video in private dwellings will almost always be intrusive but circumstances under which an officer may choose to record are likely to be in response to a specific incident police are attending, in which case there will be a legitimate aim and that will be necessary and proportionate for the same reasons as outlined above.

Policy dictates that body worn video should be activated at all domestic incidents which often, by their very nature, result in police presence at a private dwelling. It is necessary and proportionate to achieve best evidence in evidence-led prosecutions.

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

☒ Yes ☐ No

Legislative changes to Police and Criminal Evidence Act 1984 PACE came into force on 31 July 2018 that allow the use of body worn video for the capture and recording of voluntary (out of custody) suspect interviews under caution under certain circumstances if authorised by the Chief Constable. The Chief Constable of Leicestershire Police has authorised this as of 11th March 2020 :-

The exceptions within PACE where this cannot be used, in brief, if a device in working order is not available, location is unsuitable, the ‘relevant officer’ determines it should not be delayed to wait for a suitable device or location to become available, the suspect or the appropriate adult objects subject to agreement by the ‘relevant officer’ or when it is deemed unsafe to use a device in a cell.

Body worn video can also be considered for covert surveillance by certain teams within Leicestershire Police, may use BWV covertly from time to time but usage will be inline with the Policies and procedures and with the appropriate authority.

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

Action Plan

1.Confirm if the BWV policy been circulated across the organisation given that we have had a recruitment drive ?

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

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 police forces have a complaints procedure and complainants are directed to the force website. The website provides details of what a complaint is, the process of how to make a complaint and how complaints are dealt with. Submission of a complaint includes completion of an 'Expression of Dissatisfaction about the Police Service' form. Upon submission of this the complaint is sent to the Professional Standards department who will conduct an impact assesment prior to allocation and progression. The complaints are managed in accordance with the Police (Complaints and Misconduct) Regulations 2020, Police (Conduct) Regulations 2020, Police (Performance) Regulations 2020, IOPC Guidance for Handling Complaints of Discrimination, IOPC Statutory Guidance 2020 and Home Office Statutory Guidance

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

Action Plan

1.Where is the evidence of consultation held and when was it ?
10. Do officers know that they have to inform the public that they are usig BWV , has the policy been circulated to new officers , or refreshed to others ?

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?

A robust governance structure is in place in relation to body worn video, with a number of key roles identified for the use of the technology. These roles are supported by robust policies and procedures in place regarding the use of the technology. All staff members receive extensive vetting before joining the organisation and then prior to being issued a device and in order to use the body worn video system the user must undertake a training input. This input focuses on what body worn video is, operation of the devices and handling of the cameras and, how to use the software (DEMS) and best practice (law, policy, procedure and national guidance). Once this input has been delivered student officers then use the devices during their training scenarios in order to familiarise themselves with it on a practical basis. The policy and procedure is kept up to date and available to all staff on the Intranet. Video clips are stored securely on the device, which is PIN protected to protect the footage in the event the camera is lost or stolen, and then once they are uploaded to the server the device is formatted. Data from the cameras can only be downloaded to a dedicated computer. Access to the software to view video clips is granted on a needs basis and only following receiving the appropriate training. Video clips are stored securely and retained in accordance with guidelines.

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

The Business lead appointed and documented on the Force Policy and on the Force BWV intranet page, is Insp 1076 Botte.

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?

Staff responsibilities around body worn video are introduced and consolidated during training prior to issuing a camera. Training is covered by question 13. Correct use of body worn video is audited by supervisors dip sampling uploaded videos and investigator's have a duty to raise any concerns they may identify from viewing videos pertinent to their

investigation.

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

16. How are we aware that staff know their responsibilites
17. How often and where is dip sampling recorded ?

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?

Body worn video is personal issue and prior to users being issued one they must have undertaken the initial training and induction as described in question 13. This involves both practical training of the device and system training on footage playback and producing copies (such as for court). There are a number of pool cameras available and in order to book one out the user must also have undergone the same training.
There have been no significant changes to the body worn video camera or system and so users have the necessary skill and knowledge upon finishing the induction. The only change has been an upgrade in the camera to the DS3 but this has not changed any functions for the user.

The training package is currently being rewritten.

The body worn video policy & procedure is updated and reviewed regularly (at least once a year) and when this is updated a latest news article can be published informing all staff of this as well as an email cascaded to all users through supervisory. The use of body worn video also forms part of other policies and procedures to ensure users remain competent in using the system eg. sudden death procedure states not to use body worn video for recording searches of the deceased and response to sexual offences states not to use body worn video to record the account due to visually recorded interviews. All force staff go through an induction process that covers data protection training and regular awareness campaigns take place internally to ensure all staff remain updated regarding privacy considerations when carrying out their roles. Training in data protection is also subject to annual refresher training. .

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?

Users are required to complete training prior to being issued with a camera, as in question 13 and 22

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?

There is no requirement to record routine interactions with the public, and entire duties and routine patrols should not be recorded.

The organisation has a recently reviewed policy on body worn video use which covers the circumstances in which it is appropriate to use, including when it is mandatory (domestic incidents and stop search)

Body worn video can be utilised in all aspects of Policing and partnership work and brings with it opportunities to offer an improved service to the public, better quality and more robust evidence in cases, behaviour modification in the presence of body worn video, victimless prosecutions, fewer assaults on Police and a reduction in the use of force (Rialto, 2013).

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

20.Clear policies and procedures in place - where are these located internally for inspection?
21.Mention of BWV policy and procedure as part of the officer induction process - where is this recorded and reviewed and by whom?

Mention of the training package for BWV currently being re written , has this been done , by who and is it live and signed off ?

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 obtained as a result of the use of body worn video is down loaded to a master database. The master database has an auto weed date of 31 days, unless an officer confirms that the data is needed for evidential purposes such as CPIA. If data is retained evidentially then force MOPI principles will be followed.

This period is proportionate to allow any subsequent investigation linked to the recording to be allocated and reviewed by the officer in the case and marked as evidential if longer retention is necessary. It is also proportionate to prevent it being deleted prior to scenarios whereby a complaint is made or a crime is reported retrospectively

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

As Above and redaction rules are utlised when providing evidence for Trial.

Images for retention are marked as “Evidential”. Evidential footage is retained for 6 years following MOPI. Other footage is automatically deleted from the server after 30 days. Any user can submit an email request to the IT department in order for them to attempt to recover and deleted footage but in practice it is only possible to recover data recently deleted. If footage has been marked for deletion then it is deleted after 30 days. This means it is deleted from all backups as well. If a video has been deleted then the reference to the footage still shows in DEMS but cannot be played but file details can be obtained to request recovery. The server that hosts all of the file data for the entire force also hosts the backups of the files that change or get deleted (there is too much data on the server to back it up to another system each night). A proportion of the total storage is used by the backups so we can recover older or deleted files, but how far back we can go depends on the rate of change of the data. As per agreed and publicised guidance – it is the responsibility of the filming officer and any subsequent officer in case to ensure any body worn video footage (including unused material) associated with a criminal investigation or police complaint is reviewed and retained in accordance with the CPIA – Criminal Procedure and Investigations Act – code of practice. As part of Digital Evidence management system, material is marked for deletion subject to the periods provided in question 30. Once passed the media is quarantined, and unable to be accessed via standard users. The footage is then subject to a review by the RRD team, prior to the full deletion of the footage.

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

32. Retention of images longer than routine period open to review ? Are they and by who and where is this recorded .

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?

Officers are aware of the rules and regulations around accessing data for a non -policing purpose.
All staff who have access to BWV also have access to the storage system and can playback clips from any user as long as it has not been 'cloaked', in which case access to that particular video is on a needs basis following a legitimate request. Training is based on role and the principle of least privilege. Access can be audited and regular reminders are issued around legitimate access to police systems for a policing purpose. The audit function is managed within the DEMS software application. All activity within the application is logged and only users with the appropriate role in the application can access the audit logs. All interactions with the DEMS system are recorded in the log. Access to cloaked videos is controlled requiring authorisation from an Inspector or above which we will log in another system and is for a specified prearranged date and time range.

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?

In relation to cyber security risks, technical measures are in place to safeguard the information we hold, including (and are not limited to) robust firewalls, routine scanning of our infrastructure and likely sources of threats, such as email. All Leicestershire Police systems go through a penetration test on an annual basis to ensure that the high level of cyber security are maintained. In relation to traditional (physical), security risks appropriate and proportionate controls are in place to safeguard the information. These measures include (and are not limited to): Utilising encrypted media – such as encrypted USB sticks, or the information being password protected (wherever possible), Utilising trackable methods of delivery (postal) and Hand Delivery
.

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

SARs are processed through the Forces Information Management Dept.Any requests for information from ANPR systems will be directed to them in the first instancel

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?

Leicestershire Police have a number of Information Sharing Agreements in place with other agencies and each request will be reviewed and processed by a relevant person. All subject access requests are processed through a disclosure officer who is the single point of contact for all sharing of information with a third party. Sharing of footage is often required as part of the criminal justice system and working copies can be supplied to the Crown Prosecution Service (CPS). Once the footage is passed to the CPS it is down to their own internal policies and procedures as to how they keep that secure and it is unrealistic for Leicestershire Police to monitor their compliance with these. Footage may also be played in Court where it can be viewed by members of the publc gallery but they will not have copies of it; the decision to play the footage is ultimately down to the presiding legal advisor or Judge. Where third parties have been captured by the recording suitable redaction should take place as part of the court compilation or release to subjects following data access request. This should be completed using specialist software and appropriately trained personnel.

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

☒ Yes ☐ No

Action Plan

At present the default setting is that any user can access any body worn video footage by simply inputting the collar number of another officer with no justification, unless the footage is cloaked after it has been uploaded. Consider adding a 'justification' reason within the DEMS software if a user is searching footage uploaded against a collar number that is not the same as the user logged in. The software is supplied by an external company any changes to this would need to be requested, considered and approved and then paid for. It is not feasible at this stage however there is a splash screen when user's log in with a data protection

36 - Is access to DEMS audited by someone , if so who and how often , where is this recorded for audit purposes?

37- The written policy on disclosure to third parties - where is this located and is it up to date , how do people request this ?

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 equipment has been appropriately hardened to safeguard any data held on the device by the supplier (Reveal), and is certified to the ISO 27001 standard. Data is encrypted to AES 256 standard, and safeguarded by PIN protection. The PIN is a universal PIN for all users within the organisation.

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

The Force Policy is reviewed and updated with any signigicant new updates on a regular basis. The training package has been revamped to keep officers up to date and the Force IT department along with a full procurement exercise was completed at the commissioning of the product. Should a specific threat be identified, a review will be undertaken to ensure their continued suitability.

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

NO

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?

Once uploaded, images cannot be interfered with once on the server. The information can be converted into an evidential "clip" but the original cannot be corrupted. The device is encrypted to AES 256 standard and is also password protected, ensuring the integrity of the information held on the device. Information stored on the devices is transferred to the Digital Evidence management System (DEMS) via a secure transfer at standalone kiosks housed within secure facilities. The download and upload of all information is encrypted utilising TLS 1.2 technology. In addition to the data on the devices officers have a responsibility to ensure physical security of their devices. Devices are subject to physical audits by supervisors and are managed through an asset management system. All staff should receive data protection training as part of their induction to the organisation

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?

Force BWV Policy

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 for BWV

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 body worn video are securely attached to officers' stab vests with the use of 'klick fast' dock. When footage is being uploaded it is detached and connected to a desktop based standalone computer within a secure police station and after the upload is complete the camera is formatted and all footage removed. If the camera was to be lost or stolen then any footage that is on the device cannot be viewed/exported due to an access code on the device. As all of the data on the device is encrypted if the device was plugged into an external machine then the data would not be readable - the data is only decrypted with the correct key when plugged into a Leicestershire Police DEMS machine,

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

52. If the BWV is lost outside in the public domain , what is the process and contingency ?

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?

Regular review of the individual use of body worn video should be conducted by the officer's supervisor as part of continuing professional development, incident specific review (such as a complaint or performance concerns) and when filing incidents. IT systems in use across the organisation, including body worn video, are subject to regular reviews to ensure they meet the needs of the business and the original purpose. Should any areas for improvement be identified, corporate mechanisms exist to ensure that work is undertaken to improve the product at the earliest opportunity. In addition, routine updates to the system take place as part of the annual IT improvement regime.

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?

Any faults are reported to the Force IT department who will contact the company REVEAL if they are not able to resolve.

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

Action Plan

54. What does this supervisor review process consist of , how often and where is it recorded for audit purposes ?

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?

Home Office publications regarding Safeguarding Body Worn Video (BWV) Data 2018 and Technical guidance for Body Worn Video (BWV) devices: CAST, 2018 Not known if any engagement was carried out with members of the public however it was supported by Chief Officers and the Government following successful trials in other police force areas (notably Hampshire as the first force to rollout the technology). The Police Federation of England and Wales also support it.

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

NO

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?

Body worn video imagery is not used with automatic facial recognition software. Although Leicestershire Police do use facial recognition within the ID Unit we do not use the live system hence we do not run body worn videos against facial recognition software. Any suspect images obtained are compared against Leicestershire's custody images for identification purposes. We do not use Live Facial Recognition for BWV.

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?

N/A for this element

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

This area is not relevant to BWV in leicestershire due to not utilising facial or vehcile recognition.