OFFICE OF THE BIOMETRICS
AND SURVEILLANCE
CAMERA COMMISSIONER

Framework Service Level Agreement

Duty to Have Regard to Surveillance Camera Code – Framework SLA for CCTV Systems

This document provides guidance and a set of recommended minimum requirements to which local authority CCTV/VSS/VSS system owners and police forces should have regard when compiling Service Level Agreements in accordance with their legal obligations under the Protection of Freedoms Act 2012.

Using this tool

This guidance has been prepared by the Biometrics & Surveillance Camera Commissioner (BSCC), the National Police Chiefs' Council (NPCC), The Public CCTV Managers Association (PCMA), the Local Government Association (LGA) and through consultation with other key organisations.

The guidance is designed to help you and your organisation develop a Service Level Agreement (SLA). It is not in itself an SLA but a tool to help you ensure you have included all the minimum requirements that would be expected to be included in an SLA. The sections that are outlined below are not exhaustive; there is no 'one size fits all SLA' and you may wish to include additional sections to agreements you already have in place or will in the future.

It should be completed in conjunction with the Surveillance Camera Code of Practice (SC Code) and its 12 guiding principles issued under the Protection of Freedoms Act 2012 and other relevant legislation such as:

General Data Protection Regulation (GDPR) & Data Protection Act (DPA) 2018;

Data Use and Access Act (DUAA) 2025

Human Rights Act 1998;

Regulation of Investigatory Powers Act 2000;

Investigatory Powers Act 2016;

Crime and Disorder Act 1998;

Terrorism Act 2000 and Terrorism Act 2006

Relevant authorities as defined by section 33(5) of the Protection of Freedoms Act 2012[1] must have regard to the SC Code when operating surveillance camera systems and also when working with organisations who are not directly bound by that duty. Further advice on the extent and implications of that duty can be obtained from your statutory Monitoring Officer (either from the relevant local authority or the elected local policing body for a police force).

An effective SLA is a crucial part of any partnership working arrangements between organisations. This template has been designed specifically for partnerships between relevant authorities regarding the operation of surveillance camera systems. However, it will be of use for any partnership working.

The Senior Responsible Officer for compliance with Protection of Freedoms Act 2012 requirements in relation to the SC Code should oversee the completion of this document with input from other relevant people in your organisation. For example, you should seek guidance from your Data Protection Officer (DPO) for those sections of the SLA that relate to data protection issues. Furthermore, relevant authorities could have regard to standards such as BS-7958 – Video Surveillance Systems (VSS), Management and Operation Code of Practice.[2]

[1] Relevant authorities may include local authorities, combined authorities, and mayoral public authorities with responsibility for video surveillance systems (VSS), together with other key stakeholders as appropriate.

[2] BS7958 applies to CCTV/VSS schemes used in public places such areas where the public are encouraged to enter or have a right to visit, such as town centres, shopping malls, public transport, health establishments, etc; schemes that overlook a public place, such as traffic monitoring schemes; and private schemes where a camera view includes a partial view of a public place.

It should be completed with regard to the following 12 guiding principles within the Surveillance Camera Code of Practice.

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.**

2. **The user 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.**

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.**

4. **There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.**

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.**

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.**

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.**

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.**

9. **Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.**

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.**

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.**

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.**

Elected Local Authority and Policing body who will be the owner of the system and assets	
Name of organisations party to this agreement	
Scope of surveillance camera system/s covered by this agreement.	
Senior Responsible Officer Local Authority	
Senior Responsible Officer Police Force	
Signatures	
Date of sign off	
Date of review (Recommended as a minimum every 2 years)	

Section 1

Information Sharing Agreement (ISA) between the parties. This section must be completed in consultation with your Data Protection Officer (DPO).

1. Have you clearly identified the purpose(s) for which the system is to be used?

   Yes ☐

   No ☐

2. Have you clearly identified the lawful basis for your proposed use of surveillance?

   Yes ☐

   No ☐

3. Have you stated in your Information Sharing Agreement what data will be shared, how and with whom?

   Yes ☐

   No ☐

4. Have you articulated how the arrangements comply with UK GDPR & Part 3 of the Data Protection Act 2018, if personal data is being processed for law enforcement purposes?

   Yes ☐

   No ☐

5. Have you agreed the point at which Data Controllership is passed from the system owner to the investigating authority? For example, the police force will be the controller once they have received the data, and this must be formalised in the ISA. The local authority would be data controllers for the 'original' data if they continue to retain it and there are circumstances where both might be the controller.

   Yes ☐

   No ☐

6. Are there any other agreements or protocols in place regarding your CCTV/VSS system, and if so are they compatible with the SLA? For example, Overarching Information Sharing Agreements and Data Protection Impact Assessments.

   Yes ☐

   No ☐

7. Have you ensured that all staff engaged in the monitoring of CCTV are compliant with the licensing requirements of the Private Security Industry Act 2001?

   Yes ☐
   No ☐

Notes

Changes to the training you need for an SIA licence - GOV.UK

Section 2

Directed Surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA)
The Investigatory Powers Commissioner's Office (IPCO) recommends that there is a written protocol between the law enforcement agency and local authority if surveillance cameras are to be used for directed surveillance. Where appropriate the protocol should include a requirement that the local authority should see the authorisation, redacted if necessary and only allow its equipment to be used in accordance with it. This section should be completed in consultation with your RIPA Authorising Officer. (Counter Terrorism Surveillance is dealt with in section 3)

8. Do you have a written protocol with the police which satisfies you as the Data Controller and Data Owners that any directed surveillance is lawful, proportionate, and necessary?

   Yes ☐

   No ☐

9. Do both parties have a Single Point of Contact (SPOC) to help facilitate communication with regard to RIPA?

   Yes ☐

   No ☐

10. Are there suitable arrangements which can be put in place for the police to carry out directed surveillance without interfering with the normal operations of the control room?

    Yes ☐

    No ☐

11. Are there arrangements to supply feedback to the local authority once the operation has concluded and to ensure that directed surveillance is not continued beyond the validity of an authorisation under RIPA

    Yes ☐

    No ☐

12. How long do you keep your Directed Surveillance Authorisation documentation for?

Notes.

Examples of RIPA documentation.

Section 3

Counter Terrorism Surveillance.

Arrangements with Counter Terrorism (CT) units should be covered by a separate Memorandum of Understanding (MOU) to section 2 of this document. The system owner and data controller must be satisfied that any surveillance is lawful and has been expressly authorised by the appropriate authorising officer in accordance with the Regulation of Investigatory Powers Act 2000.

13. Do you have an MOU with your local Counter Terrorism unit and is this documented in the SLA?

    Yes ☐

    No ☐

14. Have you documented in the SLA how images/data/video analytics will be accessed/shared?

    Yes ☐

    No ☐

15. Have you consulted with your DPO and completed the relevant section of your Data Protection Impact Assessment?

    Yes ☐

    No ☐

16. Do you have a Single Point of Contact (SPOC) within Counter Terrorism?

    Yes ☐

    No ☐

17. Are there arrangements to supply feedback to the local authority once the operation has concluded and to ensure that directed surveillance is not continued beyond the validity of an authorisation under RIPA

    Yes ☐

    No ☐

Notes

Validation may be required by IPCO when inspecting Local Authorities for RIPA compliance. Feedback can be in the form of generic information showing the contribution of LA CCTV/VSS to the CT Strategy. The Local Authority SPOC should contact their local CT office to agree procedures and compliance with this section.

This will also help facilitate future partnership working, feedback and training which is covered in the National Counterterrorism Security Office (NaCTSO) guidance:
Working with counter terrorism security advisers

In addition, where a LA CCTV video management system has video analytics enabled for live tracking/identification, this should be included in the MOU.

Section 4

Vetting.

To help facilitate the sharing of information for the purposes of the prevention and detection of crime and public safety, Local Authority staff should be vetted to the nationally agreed minimum standard of **NPPV Level 2 (Abbreviated)**.

18. Have all your staff been vetted to the nationally agree minimum standard?

    Yes ☐

    No ☐

19. Have you included a point of contact for vetting in the SLA?

    Yes ☐

    No ☐

20. Have you included an agreed timescale for vetting results?

    Yes ☐

    No ☐

21. Do you have locally agreed protocols in the event that any staff fail vetting?

    Yes ☐

    No ☐

22. Please detail any areas where further action is required to conform more fully with the requirements of vetting.

23. Please detail any other forms of screening which you carry out for your LA staff. e.g. BS7858: Screening of individuals working in a secure environment.

Notes

Some police forces may experience significant delays with processing vetting applications. Warwickshire Constabulary offer a Police National Contractors Vetting service which includes a completion time service level agreement.

About the Police National Vetting Service | Warwickshire Police

Security Cleared Jobs Community | Police vetting levels explained: What you need to know

For cost considerations see new-rates-for-vetting-as-of-1st-april-2025.pdf

Section 5

Airwave.

Allowing local authority staff-controlled access to Airwave assists with effective, real time information exchanges with the police, benefit public and police safety and help to prevent and detect crime and comply with their requirements under the Operational Communications in Policing (OCiP) Airwave Codes of Practice.

24. Does the local authority have access to Airwave Radio?

    Yes ☐

    No ☐

25. Has the owner of the CCTV/VSS System registered with Ofcom and completed a Tetra Encryption Algorithm (TEA 2) licence?

    Yes ☐

    No ☐

26. If your staff are contracted to provide CCTV/VSS monitoring does their employer have a TEA2 Sharers Licence?

    Yes ☐

    No ☐

27. Have you documented in the SLA the measures that are in place to ensure the security of the Airwave equipment and the security of the data transmitted from this equipment?

    Yes ☐

    No ☐

28. Please detail any areas where additional action is required to conform more fully with the requirements of the TEA2 licence.

Section 6

Police Force Feedback to LA.

Where local authorities provide the police or other agencies with images or other information derived from the use of their surveillance camera systems, the police or other agency should ensure that they have effective processes in place to inform the local authority as to the outcome of their operational and/or investigative activity. This should include any judicial outcome. This will help the system managers to justify the pressing need for the surveillance system and the continued financial investment in it.

29. Are there documented Single Points of Contact in the police who can provide the local authority with feedback operationally, strategically and with regard to directed surveillance?

SPOC for day-to-day operational demands – Neighbourhood Policing Team (NPT) & Response

Yes ☐

No ☐

SPOC for strategic meetings concerning the CCTV/VSS System

Yes ☐

No ☐

SPOC for Directed Surveillance

Yes ☐

No ☐

SPOC for Counter Terrorism

Yes ☐

No ☐

30. Have you documented how the police will provide locally agreed performance indicators and feedback between the parties on at least a monthly basis?

Yes ☐

No ☐

31. Are local authority staff included in any police recognition or award schemes?

Yes ☐

No ☐

32. Have you agreed to provide the LA SPOC with statistical data on an annual basis relating to crime and anti-social behaviour in the vicinity of LA CCTV/VSS cameras?

Yes ☐

No ☐

33. Have you agreed to provide feedback to the LA SPOC regarding the quality of images reviewed during investigation or live images detailed in Section 8?

Yes ☐

No ☐

Notes

e.g. attached is an example of statistical data provided to the local authority by the police detailing crime and anti-social behaviour within the area of CCTV/VSS cameras.

Section 7

Local Authority Key Performance Indicators (KPIs).

A suite of transparent and accountable performance standards and information criteria that local authorities can make available to the public and key partners.

34. Do you have a set of key performance indicators which is provided to the police?

Yes ☐

No ☐

35. Does the SLA set out how KPIs will be made available to the public and key partners?

Yes ☐

No ☐

36. Please detail any other reports relating to the performance and effectiveness of your system.

Notes

Some suggested examples of Local Authority Key Performance Indicators could include (but are not limited to);

- total Incidents recorded by VSS (proactive and reactive),
- incidents generated from call sources such as police, shops, licensed premises,
- number of arrests captured on camera, number of footage reviews conducted,
- number of footage files downloaded/exported as evidence
- Or any other agreed minimum standards by the local authority that are suitable to the local context.

Section 8

Provision of live CCTV/VSS images by local authorities.

Wherever possible, local authorities should assist the police by providing live images of CCTV/VSS paying due regard to evidential relevance and data minimisation under UKGDPR, Data Protection Act and DUAA. This will help the police to assess an appropriate response to incidents and consider public and officer safety.

37. If the local authority provide access to live images/video analytics is this documented in the SLA?

    Yes ☐

    No ☐

38. If the local authority allows police control of their cameras is this documented in the SLA?

    Yes ☐

    No ☐

39. Does the SLA contain provisions for the police to provide audits which clearly set out the legitimacy and justification for seeking access, l along with an audit log indicating who has accessed and/or controlled the CCTV/VSS camera system?

    Yes ☐

    No ☐

40. Have you completed the relevant section of the Data Protection Impact Assessment which covers the sharing of live images?

    Yes ☐

    No ☐

Notes

Example of a camera sharing agreement between local authority and police.

Biometrics & Surveillance Camera Commissioner DPIA template and guidance.

In addition, where a LA CCTV video management system has video analytics enabled for live tracking/identification, this should be included in the SLA where it assists investigations.

Section 9

Training.

In addition to the training provided by the system owner it is recommended that the police assist local authority staff with specific training in evidential procedures, legislation, how to obtain best evidence, continuity and radio communications. In addition, it is recommended that TRIM (Trauma Risk Management) training where available is provided for incidents where trauma may be experienced.

41. Does the SLA document what training provisions the police provide for CCTV/VSS operators? For example, practical use of CCTV/VSS, legislation, Airwave, evidential and operational continuity and human rights/legitimate expectations?

    Yes ☐

    No ☐

42. Do you have a training review process established to ensure your staff are up to date with relevant legislation and guidance?

    Yes ☐

    No ☐

Notes

E.g.

Home - SCR Course

https://www.npsa.gov.uk/CCTV/VSS

https://www.marchonstress.com/page/p/trim

Section 10

Welfare.

Local authority staff are often called upon to monitor live incidents or review recordings which are graphic, disturbing and upsetting. There is also the added pressure that, apart from the ability to monitor and summon help, the operator is left in a situation of feeling unable to prevent serious injury or death. It is imperative to include LA staff in any initial debrief.

43. Does the SLA contain details of arrangements provided to ensure that LA staff are involved in the initial debrief and initial instigation of welfare support and signposted to LA SPOC?

    Yes ☐

    No ☐

44. Does the SLA document record, either joint or individual, risk management provisions?

    Yes ☐

    No ☐

Documents to be read and understood as forming part of this SLA: -

Joint LA/Police Information Sharing Agreement

LA Data Protection Impact Assessment.

Tetra Encryption Algorithm (TEA 2) license

LA Information Security Incident Reporting Policy

The Police/PCC's Information Security Incident Reporting Policy.

ICO CCTV/VSS and video surveillance guidance

BS7958

BS7858

CT MOU

LA Key Performance Indicators Document

Force vetting policy

MOPI Guidance

Digital investigations: Digital imaging and multimedia procedure - GOV.UK

Recovery and acquisition of video evidence - GOV.UK

NPCC Framework for Video Based Evidence