Surveillance Camera Commissioner

Self-Assessment Tool – Enfield Public Safety Centre (EPSC) system

LB Enfield responses **– for publication on Enfield Council website**

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 will help you and your organisation identify if you're complying with the principles in the code.

The self-assessment is for you to satisfy yourself and those that you surveille that you meet the principles and identify any additional work to show compliance.

This is the first edition of the self-assessment tool which will evolve over time.

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. Have you translated principle 1 into clear objectives? YES

If so what are they?

Prevention and detection of Crime and Disorder and public safety to assist in the overall management of LB Enfield and other public areas within client base to enhance Community Safety.
To assist the borough in its Enforcement and Regulatory functions
To assist in Traffic Management and Enforcement within the borough
Civic Building and staff and public safety
To support Civil Proceedings
Staff Administration
Automated Number Plate Reading (ANPR) connected to the police national ANPR database and Metropolitan Police system

2. Do you regularly review the system and assess against the objectives? YES

3. Have you considered the requirement of the end user? YES

4. Is the system being used for any other purpose other than those specified? NO

If so please explain

5. Have you identified any areas where further action is required more fully conform to the requirements of Principle 1? NO

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. Do you review your system annually? YES

2. Have you conducted a privacy impact assessment? (The ICO has produced a PIA code of practice and the SCC has a template you can use if required) YES
3. Do you publish your privacy impact assessment and annual review? NO

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

Action plan

1. ***System Privacy Impact to be published on council Website***
2. ***Improve our information on our web site***

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.

1. Does signage exist highlighting the use of surveillance cameras? YES

2. Does the signage highlight the point of contact? YES

3. Has there been proportionate consultation and engagement with the public and partners to establish that there is a legitimate aim and a pressing need for the surveillance camera system?

YES

4. Is the surveillance system a proportionate response? YES

5. Does your publication of information include the procedures and safeguards that are in place, impact assessments undertaken, performance statistics and other management information?

YES

6. Do you have a complaints procedure in place? YES

7. Do you make the public aware of how to escalate complaints? YES

8. Is there a defined time scale for acknowledging and responding to complaints and is this conveyed to the complainant at the outset? YES

9. Do you publish the number and nature of complains received? YES

10. Have you identified any areas where further action is required to more fully conform to the requirements of Principle 3?

Action plan

- ***Camera type PIA documents are under development with the SCC and will be completed for each type of camera on the system. This will also be published on the website***

Principle 4

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

1. What arrangements are in place to provide clear responsibility and accountability?

- ***All information is logged and has an audit trail which can be accessed if required and when requested.***
- ***There are clear documented procedures to review, download and handover of data (evidence) including documentation.***
- ***All staff are SIA licensed, police vetted and BS 7858 vetted and fully trained and attend BTEC level training courses that include DPA and Human Rights awareness.***
- ***All data systems are user and password protected, with resilience and data security measures in place.***

2. Are all staff aware of their responsibilities? YES

3. Please explain how you ensure the lines of responsibility are adhered to.

- ***All remote CCTV sites servers are locked down to live viewing only and recorded data access is only through the Enfield Public Safety Centre and its central processes.***
- ***All systems are password protected at various management levels and are able to provide an audit trail of data handling and incident and evidence documentation is retained.***
- ***Police provide resources for all criminal incident and evidence data requirements – Booking in-process is in place. Other data requests are dealt with by nominated council or cleared security staff.***

4. If jointly owned, is it clear what each partner organisation is responsible for and what the individual obligations are? YES

5. Have you identified any areas where further action is required to more fully conform to the requirements of Principle 4?

Action plan NONE

<u>Principle 5</u>

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.

1. Do you have clear policies and procedures which help ensure that any legal obligations affecting the use of such a system are addressed? YES

If so please specify.

- ***Forms and documentation are in place for operational use of the system as well as system Codes of Practice and procedure manuals for all data and evidential uses.***
- ***Fault management system in place with term CCTV contractor to maintain the system***
- ***Evidence management procedures in place***
- ***Directed Surveillance (RIPA) procedure in place and adherence to DPA and FOI as per Council policies***
- ***Staff training on Directed Surveillance, Data Protection Act and other legislation in place***

2. Do you follow a quality management system? YES

If so please specify.

- ***The EPSC has acquired British Standard BS5979 certification for secure handling of alarms and video alarm systems as well as BS 8484 for Lone Worker with UKAS accredited SSAIB Inspectorate and audited annually.***
- ***The EPSC has acquired British Standard BS 7958 for Control Room Operations and Management Standards with UKAS accredited SSAIB Inspectorate and audited annually.***

3. Are the rules, policies and procedures part of an induction process for all staff? YES

4. How do you ensure that all system users remain up to date and efficient with relevant operational, technical, privacy considerations, policies and procedures?

- ***Regular staff refresher training programmes are imbedded in our staffing contract to ensure compliance. Six months training induction of staff required as well as BTEC course programme.***

5. Have you considered qualifications relevant to the role of the system users, such as the National Occupational Standard for CCTV operations or other similar? YES

6. If so, have any of your system users undertaken any occupational standards to date? YES

7. Do your system users require SIA licenses? YES

8. If staff do not need a license, how do you ensure they have the necessary skills and knowledge to use or manage the surveillance system?

- ***All EPSC security contracted staff must have a valid SIA license to operate the system. This is one of the requirements upon employment that is managed by the contractor.***
- ***LBE EPSC staff undergoes specialist technical and operational training and obtain a SIA license and staff are additionally BS 7858 vetted and also police vetted by the Metropolitan Police Service.***

9. Have you identified any areas where further action is required to more fully conform to the requirements of Principle 5? NO

<u>Principle 6</u>

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.

1. On what basis are images retained and for how long?

- ***Street camera footage retention period is 31 days. Civic Buildings (internal) are retained for a minimum of 14 days but up to 31 days maximum depending on risk.***
- ***HD Camera retention period is up to 14 days***
- ***All images are digitally stored on secure network servers and data overwrite automatically after the set retention period unless required and downloaded within the retention period of the camera/site.***

2. Do you have an auditable process for reviewing images and managing their retention? YES

3. Are there any time constraints in the event of the enforcement agency not taking advantage of the opportunity to view the retained images? YES

4. Are there any time constraints which might affect external parties from viewing the images? YES

5. 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 official third parties? NO

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

Action plan NONE

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.

1. Do you have a policy on who has access to the stored information? YES

2. Do you have a policy on disclosure of information? YES

3. What checks do you have in place to ensure that the disclosure policy is followed?

- ***All systems have an audit trail and user passwords and user access is set at various levels.***
- ***No data is released or viewed until evidence documentation is completed and/or signed.***
- ***Clear processes and procedures are in place for evidence handling and hand over of data.***

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

Action plan NONE

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.

1. What approved operational, technical and competency standards relevant to a surveillance system and its purpose does your system meet?

- ***The EPSC has obtained BS 5979 CAT2 certification status for Alarm Receiving and Security of premises through UKAS accredited Inspectorate.***
- ***Staff are vetted to BS 7858 and SIA licensed and additionally police vetted as well.***
- ***Maintenance contractor installs to IEC and BS Standards***
- ***The EPSC has obtained BS 8484 certification status for Lone Worker monitoring services through UKAS accredited Inspectorate.***
- ***EPSC ha obtained certification to BS 7958 for CCTV Management and Operations through UKAS accredited inspectorate.***

2. How do you ensure that these standards are followed appropriately?

- ***Quality standards of operation are embedded in the councils tender processes for supply of security contractors and CCTV maintenance contractors to comply with and contract performance meetings conducted.***

3. What steps are in place to secure certification against the approved standards?

- ***All service operational standards are obtained through UKAS accredited Inspectorate certification processes and are independently audited annually for compliance to the standards.***

4. Have you identified any areas where further action is required to more fully conform to the requirements of Principle 8?

Action plan NONE

Principle 9

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

1. What security safeguards do you have in place to ensure the integrity of images and information?

- ***All systems are password and user access protected and all network systems have relevant network security e.g. firewalls etc. Resilience is also in-built in to the design of the network.***
- ***Data servers are locked down and in secure rooms***
- ***Network and system monitoring software is used to manage the data and network security***
- ***Staff training on security and DPA and other legislation is carried out***

2. If the system is connected across an organizational network or intranet, do sufficient controls and safeguards exist? YES

3. What is the specified purpose for which the information are being used and accessed and is this consistent with the stated purposes?

- ***All purposes specified in Section 1 of this assessment are used and accessed.***

4. Do you have preventative measures in place to guard against misuse of information and images? YES

5. Are your procedures and instructions and/or guidelines regarding the storage, use and access of surveillance system information documented? YES

6. Have you identified any areas where further action is required to more fully conform to the requirements of Principle 9?

Action plan NONE

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.

1. Does your system have a review process that shows it still addresses the needs and delivers the benefits that justify its use? YES

2. Have you identified any cameras that do not remain justified in meeting the stated purpose(s)? NO

3. Have you conducted an evaluation in order to compare alternative interventions to surveillance cameras? NO

If so please provide brief details.

- ***All incident and other performance data are completed on each shift and collated and evaluated monthly and annually at meetings.***
- ***The level of incidents and arrests are regularly monitored and reported and statistical analysis of staff and system performance including fault management recorded, collated and evaluated monthly and annually at meetings.***

4. Is it cost effective to continue running your surveillance camera system? YES

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

Action plan

- ***To expand and improve on our existing Independent inspection scheme to now also include oversight of compliance to the Protection of Freedoms Act 2012***

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.

1. Are the images and information produced by your system of a suitable quality for the criminal justice system to use without enhancement? YES

2. 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 required for it to be used for evidential purposes?

- ***All images are set to a high resolution and all equipment is regularly serviced and maintained by term contractors***
- ***Police are familiar with the system type that is currently used and procedures designed to further enhance their ease of acquiring required data are in progress.***
- ***Use of best practice design and integration standards is used to improve system functions and compatibility and access by prosecuting agencies and other users.***

3. Do you have safeguards in place to ensure the forensic integrity of the images and information including a complete audit trail? YES

4. Do you have a policy on data storage, security and deletion? YES

5. Is the information stored in a format that is easily exportable? YES

6. Does the storage ensure the integrity and quality of original recording and the Meta data? YES

7. Have you identified any areas where further action is required to more fully conform to the requirements of Principle 11?

Action plan NONE

NONE

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.

1. Do you use any specialist technology such as ANPR, facial recognition, Body Worn Video (BWV) or remotely operated vehicles (Drones)? YES

If so, please specify.

- ***ANPR is currently in use in the borough and is linked directly to the Metropolitan police ANPR system that is connected to National ANPR Data Centre (NADC) for crime and monitoring purposes.***
- ***No ANPR data sent to the police is held by the EPSC, it is transmitted to the police for their National police DPA retention policy and usage.***
- ***Morson Road Depot has an ANPR system to manage the security access and egress of the site and then the data overwrites automatically after a set period.***

2. Do you have a policy in place to ensure that the information contained on your database is accurate and up to date? YES

3. Do you have a procedure for deciding when and whether an individual or vehicle should be included in a reference database? YES

4. What policies are in place to determine how long information remains in the reference database?

- ***All ANPR data is sent directly to the MPS who have to comply with National police and ACPO guidance on ANPR data usage.***
- ***Site Depot ANPR is kept for a designated period for performance monitoring purposes and security audits. They are then overwritten automatically.***

5. Are all staff aware of when surveillance becomes covert surveillance under the Regulation of Investigatory Powers Act (RIPA) 2000? YES

6. Have you identified any areas where further action is required to more fully conform to the requirements of Principle 12?

Action plan

NONE