DPIA: Public Space Surveillance CCTV System

Submitting controller details:

Name of controller	Charnwood Borough Council
Subject/title of DPO	CCTV and Enviro Crime Manager
Name of controller contact	Nicola Gibson

Step 1: Identify the need for a DPIA.

1. Identify why your deployment of surveillance cameras requires a DPIA

Public Monitoring

Service aims:

The images and audio will be used:

- To make Charnwood a safe and clean place in which to live, work and visit
- To reduce anti-social behaviour, youth nuisance, drug and alcohol misuse and provide public reassurance
- To gain evidence of environmental crimes such as graffiti, vandalism, littering and fly-tipping
- To ensure that traffic flows easily and safely through the town's streets by providing information to the media and public
- For the prevention and detection of crimes
- To provide assistance and direction for pre-planned events and operations or in the event of a major emergency
- To gain evidence for use in court proceedings.

Type of Processing:

The camera will start to record when it detects motion, so if a vehicle stops within the camera capture area, it will record the vehicle details so that a registered keeper check can be completed using the link provided by DVLA.

Litter Enforcement Camera:

The camera will detect the arc that deposited litter makes when it leaves the vehicles, this event will be recorded, and the vehicle registration number will also be recorded to enable a DVLA search for the registered keeper details to issue a penalty notice.

Supporting documents to read alongside this DPIA:

2. What are the timescales and status of your surveillance camera deployment?

The system is an existing town centre system monitored, maintained and run in accordance with the Surveillance Commissioners Code of Practice. and governing guidance.

GDPR Article 6(1)(e): Processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller.

Step 2: Describe the processing

3. Where do you need to use a surveillance camera system and what are you trying to achieve?

CCTV cameras have been installed in areas of the town centres and public places to assist in:

- the prevention or detection of crime
- the apprehension or prosecution of offenders
- the assessment or collection of a tax or duty or an imposition of a similar nature
- Public safety and safeguarding

Information is collated from local crime and anti-social behaviour statistics which are provided by the Police and monthly records produced by the CCTV control room which detail:

- reactive and proactive incidents
- Incidents monitored by subject
- arrests recorded on camera,
- reviews of footage and the production of evidence.

4. Whose personal data will you be processing, and over what area?

The council will process personal data of persons in public places such as town centres, parks, car parks, and certain residential streets. The data collected and processed is in the form of recorded video footage.

There will be images of children, vulnerable persons, people from minority ethnic groups and religious beliefs however this will not be known at the time of recording unless the cameras are being proactively used by staff. Any proactive monitoring of the public must be justified by the operator. A full record of incidents is maintained and inspected by the system manager on a regular basis.

Images of individuals will only be released to investigating authorities in accordance with the objectives listed in the code of practice and upon a signed DPA form. The system will be used in an overt manner and signage informing the public that CCTV is in operation will be displayed throughout the borough.

The CCTV system does not discriminate in any way, nor does it have any analytical software which could be used to discriminate people.

5. Who will be making decisions about the uses of the system and which other parties are likely to be involved?

The data owner and data controller is Charnwood Borough Council. The council will share data with:

1. Statutory prosecuting authorities

2. Clients and authorised investigators

3. Partners concerning safety of children and vulnerable adults

No other organisation will have access to the data other than general individuals exercising their rights in relation to subject access requests.

6. How is information collected?

Fixed CCTV

Redeploy able CCTV

7. Set out the information flow, from initial capture to eventual destruction.

Data will be captured in video format. The system is a combination of hard wired, wireless point to point and 3/4G transmission. There is live monitoring by SIA Licensed CCTV operators from the main CCTV control room.

There is no AFR or audio recording. Staff will be provided with intelligence by the police relating to crime hotspots, wanted and missing persons. The retention period is 28 days after which there is an automatic deletion of the footage.

Procedures, data sharing and security are in line with Council policy and procedures. Authorised staff have received relevant training in legislation, procedures and use of the system.

Footage may be retained as a master tape in an evidence locker for more than 30 days. e.g. major incident where a large amount of data has been retained for investigation. Civil Proceedings, Subject Access Requests, staff training and HR investigations.

The evidence locker is reviewed by the manager on a monthly basis. The principles of GDPR/DPA 2018 will be adhered to at all times.

8. Does the system's technology enable recording?

Yes

If recording is enabled, state where it is undertaken (no need to stipulate address, just Local Authority CCTV Control room or on-site will suffice for stand-alone camera or BWV), and whether it also enables audio recording.

Local Authority CCTV Control Room

9. If data is being disclosed, how will this be done?

- Only by on-site collection following receipt of signed DPA form
- Copies of footage released (detail method below)

Police/statutory prosecuting authorities will access data on site.

Subject Access requests, requests from Insurance Companies and solicitors will be dealt with using encrypted media and courier or recorded delivery. All parties are required to sign a disclosure form for any media.

10. How is the information used?

- Monitored in real time to detect and respond to unlawful activities
- Monitored in real time to track suspicious persons/activity
- Used to search for vulnerable persons
- Used to search for wanted persons
- Recorded data disclosed to authorised agencies to support post incident investigation, including law enforcement agencies
- Recorded data disclosed to authorised agencies to provide intelligence Other (please specify)
- Released to council departments investigating ASB, Licensing and Fly Tipping.

Step 3: Consultation process

11. Record the stakeholders and data subjects you have consulted about the deployment, together with the outcomes of your engagement.

Consultation carried out at commencement of service in 2008

Step 4: Assess necessity and proportionality.

12. What is your lawful basis for using the surveillance camera system?

GDPR Article 6(1)(e): Processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller.

Local authorities establish their CCTV systems under the GDPR/DPA 2018 and Section 17 Crime and Disorder Act 1998 which places an obligation on local authorities and the Police to work in partnership to develop and implement a strategy for tackling crime and disorder.

Section 17 outlines how and why local services may impact on crime and disorder and indicates the reasonable actions that might be put in place to ensure a co-ordinated approach to crime reduction. Evidence shows the opportunity for crime and disorder may be reduced and the safety and reassurance of the public improved when there is adequate CCTV coverage, and it is used with other interventions.

Using CCTV remains a strategic, financial and operational choice in exercising crime reduction partnership responsibilities between the Police and other relevant supporters. In addition, Section 163 of the Criminal Justice and Public Order Act 1994 creates the power for local authorities to provide closed circuit television coverage of any land within their area for the purposes of crime prevention or victim welfare

13. How will you inform people that they are under surveillance and ensure that they are provided with relevant information?

Letters circulated to residents prior to the installation of deployable cameras. Charnwood Borough Council website provides information on location of cameras, statistics, privacy notice. Surveillance Camera Commissioner Self-Assessment Tool (this document), Code of Practice and Data Protection Impact Assessment.

Appropriate signage in and around the area where surveillance is taking place

14. How will you ensure that the surveillance is limited to its lawful purposes and the minimum data that is necessary for those purposes?

Charnwood Borough Council has installed CCTV (Closed Circuit Television) cameras in various locations within the Borough for the purposes of reducing crime, disorder, anti-social behaviour and the fear of crime by helping to provide a safer environment for those people who live and work in the area and for visitors travelling through the area.

CCTV is also installed on highways for monitoring traffic on a temporary basis. In all locations, signs are displayed notifying the public that CCTV is in operation and providing details of who to contact for further information about the scheme.

The purpose and use of the CCTV system are to provide the Police and enforcement agencies with assistance to:

- detect, deter and prevent crime and disorder;
- to help identify, apprehend and prosecute offenders;
- to provide the Police/Council with evidence to enable criminal and/or civil proceedings to be brought to the courts; and
- to maintain public order.

Some examples of how we use your data are provided below;

• Providing evidence in criminal proceedings (police and criminal evidence act 1984 and criminal procedure and investigation act 1996)

• Providing evidence in civil proceedings

• The prevention and reduction of crime and disorder

• The investigation and detection of crime

• Identification of witnesses

Effectiveness of the system is measured in monthly performance indicators along with information supplied by the Police and other council departments.

Effectiveness of the system along with compliance with the Protection of Freedoms Act 2012 and Surveillance Commissioners Code of Practice, Compliance with the GDPR/DPA is measured through Surveillance Camera Commissioner Self- Certification process.

15. How long is data stored?

Footage is retained for 28 days and then automatically deleted unless stored in the evidence locker. This should give investigating authorities and Data Subjects sufficient time to request footage.

16. Retention Procedure

- Data automatically deleted after retention period
- Under certain circumstances authorised persons may override the retention period, e.g. retained for prosecution agency

Footage may be retained in an evidence locker for more than 28 days. e.g. major incident where a large amount of data has been retained for investigation.

Civil Proceedings, HR issues and Subject Access Requests. The evidence locker is reviewed by the manager on a monthly basis.

17. How will you ensure the security and integrity of the data?

Access is restricted to the control room and system. The system is password protected, and use is subject to regular monitoring by management.

DVD's or encrypted USB's are released to police officers, encrypted USB are released to third parties such as Insurance companies and solicitors via recorded delivery and email confirmation prior to disclosure of the encryption code. No international transfers are made.

18. How will you respond to any subject access requests, the exercise of any other rights of data subjects, complaints or requests for information?

The councils CCTV policies and procedures are fully compliant with the GDPR/DPA 2018 for general disclosure access requests and CCTV related subject access requests.

Information on subject access can be found on the Charnwood Borough council website and all requests are via an online form on the web site then passed to the CCTV Manager. Any complaints are dealt with through the council's complaints procedures.

Complaints Process - Charnwood Borough Council

19. What other less intrusive solutions have been considered?

These have not been identified but if they were to become available, they would be considered**.**

20. Is there a written policy specifying the following?

- The agencies that are granted access
- How information is disclosed
- How information is handled

There is a standard operating procedure and a Code of Practice covering all of these areas. There is also a Data Protection Impact Assessment. These documents can all be found on the Charnwood Borough Council website:

CCTV in Charnwood - Charnwood Borough Council

Step 5: Identify and assess risks.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Non-Compliance of GDPR/DPA 2018. The GDPR/DPA sets out seven key principles which LA CCTV System owners must comply with whilst operating a Public Space Surveillance System: • Lawfulness, fairness and transparency • Purpose limitation • Data minimisation • Accuracy • Storage limitation • Integrity and confidentiality (security) • Accountability Non-compliance may result in prosecution, financial penalties and severe damage to the reputation of the local authority.	Remote, possible or probable Possible	Minimal, significant or severe Significant	Low, medium or high Medium
Compliance with articles 6, 8 and 14 of the Human Rights Act. The Act applies to public authorities and other bodies, which may be public or private, when they are carrying out public functions Article 6: the right to a fair trial Article 8: right to a private and family life Article 14: protection from discrimination. A breach of any article may impede on the subjects' rights and result in the prosecution of the local authority resulting in financial penalties and severe damage to its reputation.	Possible	Significant	Medium

Compliance with Surveillance Commissioner Code of Practice and the Protection of Freedoms Act 2012. The Code of Practice is issued by the Secretary of State under Section 30 of the 2012 Protection of Freedoms Act. Relevant authorities (as defined by section 33 of the 2012 Act) in England and Wales must have regard to the code when exercising any functions to which the code relates. A failure on the part of any person to act in accordance with any provision of the surveillance camera code does not of itself make that person liable to criminal or civil proceedings. The surveillance camera code is admissible in evidence in any such proceedings. (A court or tribunal may, in particular, take into account a failure by a relevant authority to have regard to the surveillance camera code in determining a question in any such proceedings. This is reflected in the Crown Prosecution Service Disclosure Manual Reputational damage to Local Authority. The court may take inference in an authority's non-compliance.	Possible	Significant	Medium
Security of Data A Security Data breach may result in prosecution under GDPR/DPA 2018 and result in financial penalties and severe damage to the reputation of the local authority.	Possible	Significant	Medium

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Unauthorised Disclosure Unauthorised Disclosure may result in prosecution under GDPR/DPA 2018 and subject to financial penalties and severe damage to the reputation of the local authority.	Remote, possible or probable Possible	Minimal, significant or severe Significant	Low, medium or high Medium
Misuse of Data Misuse of data may result in prosecution under GDPR/DPA 2018 and subject to financial penalties and severe damage to the reputation of the local authority.	Possible Medium	Significant	Medium

Address the risks

Explain how the effects of privacy enhancing techniques and other features mitigate the risks you have identified. For example, have you considered earlier deletion of data or data minimisation processes, has consideration been given to the use of technical measures to limit the acquisition of images, such as privacy masking on cameras that overlook residential properties? What security features, safeguards and training will be in place to reduce any risks to data subjects. Make an assessment of residual levels of risk.

Note that APPENDIX ONE allows you to record mitigations and safeguards particular to specific camera locations and functionality.

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk			
Options to reduce or eliminate risk	**Effect on risk**	**Residual risk**	**Measure approved?**
Compliance with GDPR/DPA 2018. Management of the use and security of the system including monitoring, reviewing and downloading of footage. Regular audits carried out and SCC Certification achieved.	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes
Compliance with articles 4, 6 and 13 of the Human Rights Act Management of the use and security of the system including monitoring, reviewing and downloading of footage. Regular audits carried out. Spot checks on proactive monitoring by staff.	Reduced	Low	Yes
Compliance with Surveillance Camera Code of Practice and the Protection of Freedoms Act Management of system. Seek Surveillance Camera Commissioner certification.	Reduced	Low	Yes

Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved?
Security of Data Management of the use and security of the system including monitoring, reviewing and downloading of footage. Regular audits carried out. Spot checks on proactive monitoring by staff, use of passwords and checks carried out by maintenance contractors for network security.	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes
Unauthorised Disclosure Release of data is strictly controlled by the council. Data Protection Access forms used by Police for all requests. All parties who use data from the system are aware of their obligations under GDPR/DPA. Full audit trail for any release of data. CCTV staff advised and updated in team meetings and training undertaken. Regular monitoring by CCTV Team Leader on disclosed footage.	Reduced	Low	Yes
Misuse of Data Release and use of data is strictly controlled by the council. All parties who use data from the system are aware of their obligations under GDPR/DPA. Full audit trail for any release of data. CCTV staff advised and updated in team meetings and training undertaken. Regular monitoring by CCTV Team Leader on disclosed footage.	Reduced	Low	Yes
Financial Loss Compliance with GDPR/DPA, POFA, Code of Practice and operating procedures reduces the risk of unauthorised disclosure or the misuse of data. Regular audits are carried out by the system manager.	Reduced	Low	Yes

Authorisation
If you have not been able to mitigate the risk then you will need to submit the DPIA to the ICO for prior consultation. Further information is on the ICO website.

Item	Name/date	Notes
Measures approved by: CCTV Manager	Nicky Gibson 01/02/2025	DPIA and other documents to be added to website once finalised.
Residual risks approved by: CCTV Manager	Nicky Gibson 01/02/2025	If you identify a high risk that you cannot mitigate adequately, you must consult the ICO before starting to capture and process images.
DPO advice provided by:	Emily Henderson 12/12/2024	DPO should advise on compliance.
Summary of DPO advice		
DPO advice accepted or overruled by: Accepted (specify role/title)	Emily Henderson 12/12/2024	If overruled, you must explain your reasons.
Comments		
Consultation responses reviewed by: CCTV Manager	n/a	If your decision departs from individuals' views, you must explain your reasons
Comments		
This DPIA will be kept The DPO should also review under review by: CCTV Manager		The DPO should also review ongoing compliance with DPIA.

APPENDIX ONE

This template will help you to record the location and scope of your surveillance camera system and the steps you've taken to mitigate risks particular to each location. Location: Each system operator/owner should list and categorise the different areas covered by surveillance on their system. Examples are provided below.

Location type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
Town centre shopping areas, Public car parks,	PTZ Fixed	xxx	24 hours	24 hours - Regular camera patrols based upon risk and intelligence information	The privacy level expectation in a town centre and public car parks is very low. These areas have appropriate signage for CCTV, its use, purpose and contact details. All recording and evidence downloads are secure and managed by the CCTV Manager and CCTV Team Leader
Residential streets	PTZ Fixed	xxx	24 hours	24 hours - Regular camera patrols based upon risk and intelligence information	The privacy level expectation in residential streets is medium. These areas have appropriate signage for CCTV, its use, purpose and contact details. All

					recording and evidence downloads are secure and managed by the CCTV Manager and CCTV Team Leader. Privacy zones are programmed as and when required
Parks	PTZ Fixed	xxx	24 hours	24 hours - Regular camera patrols based upon risk and intelligence information	The privacy level expectation in the parks is low. These areas have appropriate signage for CCTV, its use, purpose and contact details. All recording and evidence downloads are secure and managed by the CCTV Manager and CCTV Team Leader. Regular audit checks are carried out on camera use in these areas.
Deploy able Cameras	Dome/PTZ	5	24 hours	Dependent upon type of camera. Wireless are 24 hours. Regular camera patrols based upon risk and	Dependent on the location. of deployment the privacy level can range from low to medium. Any deployment includes

				intelligence information	public consultation with members of the public being shown privacy zones programming so as to reassure them.