DP Ref: DPIA 047

Data Protection Impact Assessment for CCTV Cameras & Surveillance Devices

The Surveillance Camera Code of Practice requires the proposed use of surveillance camera systems to take into account the effect on individuals and their privacy. The best way for teams to ensure this is by carrying out a data protection impact assessment (DPIA) and allows the council as a data controller to demonstrate that its processing of personal data is compliant with the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018.

This form should be used for both internal and partnership projects which involve the use of CCTV cameras and/or other surveillance devices. The form should be completed with the assistance of the Council's Data Protection Officer.

It is important to use clear and simple language, without acronyms, to explain why the personal data is needed and how it is to be used

Service Name	Hertfordshire CCTV Partnership
Business Unit:	Communities & Neighbourhood
Lead Officer	Mike Read
Job Title	CCTV Operations Manager
Team Name	Hertfordshire CCTV Partnership
Telephone	01438 242814
Email	Mike.read@stevenage.gov.uk

1. Description of purpose of surveillance camera system

- *What's the problem(s) the surveillance system is trying to resolve?*
- *Why the proposed surveillance system is considered most effective?*
- *How will the surveillance system address the problem(s)identified?*
- *How will success will be measured (e.g. reduction in crime, fear, increased detection, etc)?*

Include evidence: e.g. crime statistics for the last 12 months, the type, location, times and number of offences, housing, community and any environment issues relevant at the time.

To provide Herts and Beds Constabulary with footage and evidence for the prosecution of offenders or incidents within the Hertfordshire & Bedfordshire area who have been caught on CCTV operated by the Hertfordshire CCTV Partnership (HCCTV).

2. Location of Surveillance Cameras *(please state specific location)*
Cavendish Road, Stevenage, SG1 1ET

3. Describe surveillance system activity *(select all which apply)*	
☐	New surveillance technology or functionality is being added onto an existing system that may affect privacy (*e.g. automatic facial recognition, ANPR, audio recording, body worn cameras, unmanned aerial vehicles (drones), megapixel or multi sensor very high resolution cameras*)
☐	Processing more sensitive data /capturing images from a different location.
☐	Introduction of new surveillance camera systems or additional technology that may affect privacy
☒	Review of existing surveillance systems to ensure it is still justified
☐	Surveillance involves cross referencing to other collections of personal information or involves third parties undertaking activities either on the council's behalf or in their own right.
☐	Changes to recorded images and information being handled, used or disclosed
☐	Increase to area captured by surveillance camera systems.

4. Is the surveillance activity driven by any legal obligation or official duties/responsibility?			
Yes	☒	Please state	The processing is necessary for compliance with the Police and Criminal Evidence Act 1984 (PACE) and Regulation of Investigatory Powers Act (2000)
No	☐		

5. Is the surveillance necessary and proportionate to the problem that it is designed to mitigate?			
Yes	☒	Please state	To monitor activities taking place in the local areas for effective crime prevention and detection
No	☐		

6. What other less privacy-intrusive solutions such as improved lighting have already been used or considered? (e.g. better lighting, physical security) Please provide reasons for not relying on these measures?	
Please state	Physical security and other alternative is not possible as it required huge amount of resources

7. What is the lawful basis for using the surveillance camera system? (Article 6,9 GDPR or Part 3 of DPA 2018)	
Please state	Non-law enforcement purposes: The processing of CCTV images is carried out by the council by virtue of its official functions under Article 6(1)(f) and considered necessary for reasons of a substantial public interest under Articles 9(2)(g) & 10 of the GDPR. The processing is also necessary for crime prevention and detection purposes and authorised under Paragraphs 2 & 10 of Part 2 to Schedule 1 of the UK Data Protection Act 2018. Law enforcement purposes The processing is necessary for the prescribed "law enforcement purposes" prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties referenced under Para 31 to Part. 3 of the Act. Where the council processes data for the law enforcement purposes they do so as a "data controller" defined under Paragraph 32 to Part.3 of the Act.

8. How is information collected			
☒	CCTV camera	☐	Unmanned aerial systems (drones)
☐	Stand-alone cameras	☐	Auto Facial Recognition
☐	Body Worn Video	☐	Audio Recording
☐	Real–time Monitoring	☐	Auto Number Plate Recognition (ANPR)
☐	Other (please specify)		

9. Where will information be collected from?			
☒	General public in monitored areas (general observation)	☐	Visitors
☐	Target individuals or activities (suspicious persons/incidents)	☐	Other (please specify)
☐	Vehicles		

10. How will information be used? (Tick all that apply)			
☒	Monitored in real time to detect and respond to unlawful activities	☒	Recorded data disclosed to authorised agencies to support post incident investigation by, including law enforcement agencies

☒	Monitored in real time to track suspicious persons/activity	☐	Compared with reference data of persons of interest through Automatic Facial Recognition software
☒	Used to search for vulnerable persons	☐	Compared with reference data for vehicles of interest through Automatic Number Plate Recognition software
☒	Used to search for wanted persons	☐	Recorded data disclosed to authorised agencies to provide intelligence
☐	Other (please specify)		

11. Has consultation been carried out with the public or stakeholders?
(e.g. local area committees, groups, forums, safer neighbourhood meetings, or surveys/questionnaires sent to residents/businesses)

Yes	☒	Please state	via public consultation prior to any camera needs to be placed
No	☐		

12(a) List the benefits to be gained from using surveillance cameras?
(e.g. Is there a need to prevent/detect crime in an area)

- Crime deterrent
- Acts as a serious deterrent to criminal activities
- Monitors activities taking place in the local areas for effective crime prevention and detection
- Collection of legally admissible evidence
- Increased public safety
- Sense of security for maintaining public confidence and trust
- Protects against potential property theft, and vandalism
- Reduces the fear of crime & anti-social behaviour
- Improves the safety and security of residents, visitors and the business community

12(b) How will the listed benefits above be reviewed to ensure the particular camera system/hardware/software/firmware remains necessary, proportionate and effective in meeting its stated purpose?

Reference to The Surveillance Commissioner's Code 12 Guiding Principles plus annual review of the DPIA.

13. List the potential risks <u>to the data subject</u> of use of their personal data from the surveillance camera system and state the likelihood and impact of the identified risks to the data subject (*Refer to Appendix A for risk assessment guide)*

Identified risks in relation to personal data **NOT** being processed in compliance with GDPR Principles (a) –(f) listed below:	State risk score for all identified risks **Impact of risk** **(e.g. Score=2)**	**Likelihood of risk** **(e.g.Score=2)**	**Overall risk level (Impact v Likelihood)** **e.g. (2 x 2)**
a) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("purpose limitation" principle)	**4**	**2**	**8**
b) adequate, relevant and limited to what is necessary in relation to the stated purposes ("data minimisation" principle) ***(e.g. unrelated individuals being recorded, risk of continuous monitoring)***	**4**	**2**	**8**
c) accurate and, where necessary, kept up to date ("accuracy" principle) ***(e.g. unusable or poor recordings/ footage not being erased)***	**4**	**2**	**8**
d) kept for no longer than is necessary for the purposes for which the personal data are processed; (except for archiving purposes in the public interest, scientific or historical research or statistical purposes with use of appropriate safeguards to protect data) ("storage limitation" principle) ***(e.g. recordings being kept longer than is required)***	**3**	**2**	**6**
e) processed in a manner that ensures appropriate security and protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality') ("security" principle) ***(e.g. lack of security to prevent unauthorised access or use of recordings)***	**4**	**2**	**8**
f) compliant with all the Principles and evidenced ("accountability" principle) ***(e.g. lack of proper guidance regarding handling of recordings by staff and third parties)***	**4**	**1**	**4**
g) Risk of intrusion to privacy & collateral intrusion	**4**	**2**	**8**

h) Interference with ECHR human rights and freedoms ***(e.g. right to private & family life, conscience & religion, expression or association)***	**4**	**1**	**4**
i) Potential discrimination/ disproportionate impact upon particular sections of the community ***(e.g. religious/ethnic)****?*	**4**	**1**	**4**

14(a) State measures taken to reduce <u>medium/high</u> risks identified above ?

Measures:	Outcome *(Is the risk removed, reduced or accepted)*
A. Purpose Limitation Principle Ensure collected recordings is used only for the related purpose and not used for any other purpose	Reduced.
B. Data Minimisation Principle Use only the minimum amount of information and share and record only relevant details.	Reduced.
C. Accuracy Principle Check the cameras are kept in fully working order and to operational standards	Reduced.
D. Storage Limitation Ensure all the recordings are deleted according to CCTV retention guidance	Reduced.
E. Security Principle Only authorised staff & SIA license officers will have access to the information	Reduced.
F. Accountability Principle The public will be informed and made aware that CCTV is in the area with clear signage in place and on the Herts CCTV Partnership. website and privacy notice.	Accepted.
Ensure that all data shared with other parties are done so using a Subject Access Request document.	Reduced.
G. Risk of Intrusion to Privacy & Collateral Intrusion: The positioning of cameras will not be focused on private spaces or directly on private properties.	

14(b) For measures identified in (a) above state if already implemented, or expected timeframe for implementation

All are already implemented.

15. Have any data protection by design and default features been adopted to reduce privacy intrusion? Could any features be introduced as enhancements? *(e.g. privacy masking on camera that overlook residential properties)*			
Yes	☒	Please state	Pixilation is used for private properties
No	☐		

16. Do the images need to be able to recognise or identify individuals, or could the purpose be met using images in which individuals cannot be identified?
Yes.

17. List all organisations that will be using data derived from the surveillance camera?
Herts & Beds Police Authority and HCCTV partners: Stevenage Borough Council, East Hertfordshire District Council, North Hertfordshire District Council and Hertsmere Borough Council.

18. Have you told the individuals subject to surveillance how and why their personal data will be used? *(e.g. privacy notices, prominent signs, media /publicity campaign)*		
Yes	☒	Via visible signs in designated areas and on the Herts CCTV Partnership website and privacy notice
No	☒	In circumstances where the purpose of the data processing is for crime prevention and detection purposes as prescribed under Paragraphs 2 and 10 of Part 2 to Schedule 1 of the UK Data Protection Act 2018, and communicating the data processing taking place to the data subject (e.g. suspect) would prejudice criminal investigations.

19. If no, are you going to tell them?			
Yes	☐		
No	☒	Why not?	Not where the purpose of the processing is for crime prevention and detection, and communicating the data processing would compromise ongoing investigations. There are prominent signs located in various public areas notifying the public that CCTV monitoring is in operation, with contact details of the data controller and further information about the data processing of CCTV images on the Herts CCTV Partnership website.

20. How will individuals be given the opportunity to exercise their data rights, complain or request for information?

Individuals can call or email us at 01438 242814 or mike.read@stevenage.gov.uk and can also contact us web site www.hertfordshirecctv.co.uk

21. How will you make sure that personal data used is kept accurate and up to date?

Continuously recording and updating is carried out on a daily basis. Recordings are overwritten after 28 days. Evidential data is held for 6 months and is audited.

22. How long will personal data be held (e.g. footage, images, recordings, etc)?
(Refer to retention guidance for assistance)

28 days according to the council's retention guidance

23. How will you make sure that you don't hold the data for longer?

Data is set to be automatically overwritten.

24. How will the data be held / stored?

In electronic format on devices locked away in a secured cabinet which is password protected and strictly access controlled

25. Where will data be stored (including back-up data)?

Location	HCCTVP Servers located at Cavendish Road, Stevenage	Country	UK only.

26. What technical security measures will be in place to protect the data?

Only authorised users can access it as it is password protected and access controlled.

27. What organisational measures will be in place to ensure that unauthorised access is prevented?

(e.g. staff operating CCTV/surveillance systems are suitably trained)

Policies & procedures are in place, regular communication and updates are shared with staff in case of any changes to prevent unauthorised access

28. How will technical and organisational security be monitored/audited?

Via the Veracity database.

29. If personal data is transferred/shared between agencies/partners how will this be achieved securely?
Yes. Transfer of data is carried out using an encrypted disc.
30. How will you ensure that third parties will also comply with data protection obligations?
Via a signed partnership data sharing agreement.
31(a) What future demands may arise for wider use of images derived from the surveillance camera system and how will these be addressed? *(e.g. Will images from the surveillance camera system be processed for other purposes e.g. facial ID, traffic monitoring/enforcement, ANPR, body worn cameras, etc)*
None are envisaged at the moment.
31(b) Does the camera system presently have a future dual function or dual purpose?

Yes	☐	Please state	
No	☒		

As lead officer, I confirm that the information recorded on this form is, to the best of my knowledge, an accurate and complete assessment of the potential privacy impacts of this service.

This DPIA will kept under review by

Michael Read

Name	Signature	Date
Michael Read		**18.05.2020.**

Please return your signed and dated form to:

Data Protection Officer
Stevenage Borough Council
Daneshill House,
Danestrete, Stevenage,
SG1 1HN
Email: **dpa@stevenage.gov.uk**

If you have any questions about the Data Protection Impact Assessment process, or if you need any help completing this form, please contact the DPO using the details above.

	Data Protection Officer use only
	DPIA has provided clear evidence of:
☒	Lawful basis for processing
N/A	Consent arrangements in place
☒	Cloud storage/remote hosting in acceptable location
☒	Sensitivity and risk to data subject sufficiently mitigated
☒	Deletion/return of data at end of project in place
☒	Sign off by project lead
N/A	Processor input
OR	
☐	Additional information requested [dd/mm/yy]

DPIA reviewed and approved by the Data Protection Officer:

Name	Signature	Date
D WILLIAMS		22/05/2020

Or

Requires further consideration by the Data Protection Officer [dd/mm/yy]

If Required

Consultation with ICO due to risk to privacy [dd/mm/yy]

ICO approved [dd/mm/yy]

ICO rejected [dd/mm/yy]

DPIA copy to be placed on Records of Processing Activities (ROPA)

Appendix A RISK ASSESSMENT

Risk Identification
When identifying potential risks or disadvantages of the processing of personal data derived from surveillance activities, such risks should consider the GDPR Principles and Surveillance Code of Practice listed below:

THE GDPR PRINCIPLES
Personal data processing must be:

a) lawful, fair and in a transparent manner ("lawfulness, fairness and transparency" principle)

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("purpose limitation" principle)

c) adequate, relevant and limited to what is necessary in relation to the stated purposes ("data minimisation" principle)

d) accurate and, where necessary, kept up to date; personal data that are inaccurate should be deleted or erased ("accuracy" principle)

e) kept for no longer than is necessary for the purposes for which the personal data are processed; (except for archiving purposes in the public interest, scientific or historical research or statistical purposes with use of appropriate safeguards to protect data) ("storage limitation" principle)

f) processed in a manner that ensures appropriate security and protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality') ("security" principle)

g) compliant with all the Principles and evidenced ("accountability" principle)

E.g. A project that involves sharing of personal data may risk being used for another incompatible purpose, with potential excessive or inaccurate processing of data when shared with third parties. The data processing therefore would risk breaching: (b) purpose limitation principle & (c) data minimisation principle detailed above.

SURVEILLANCE CCTV CODE OF PRACTICE PRINCIPLES
When using CCTV/Surveillance Devices:

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 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.

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.

E.g: A system that consists of static cameras in a residential housing block will generally present a lower risk than a system that has multiple High Definition Pan Tilt and Zoom (PTZ) cameras.

The DPIA should help identify any cameras (irrespective of the type) that may be directed at a more vulnerable area (e.g. a children's play area) and thus presenting a higher privacy risk.
It also allows the consideration of risks associated with any integrated surveillance technology such as automatic facial recognition systems, along with security measures against cyber disruption to surveillance systems.

Level of Risk

IMPACT		LIKELIHOOD			
		Rare (1)	**Unlikely (2)**	**Possible (3)**	**Likely (4)**
	High (4)	4	8	12	16
	Medium (3)	3	6	9	12
	Low (2)	2	4	6	8
	Very Low (1)	1	2	3	4

IMPACT v LIKELIHOOD = Level of risk

IMPACT	INDICATORS
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, homelessness, worsening of health etc)
Medium (3)	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear etc)
Low (2)	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem
Very Low (1)	Individual will not be affected

LIKELIHOOD	INDICATORS
Likely (4)	**Above 60%** Will probably occur at some time or in most circumstances Likely to occur at least once in the next 3 years
Possible (3)	**30% - 60%** Fairly likely to occur at some time, or in some circumstances Likely to occur at least once in the next 5 years
Unlikely (2)	**15% - 30%** Is unlikely to, but could occur at some time
Rare (1)	**5% - 15%** May occur only in exceptional circumstances Extremely unlikely to occur in the next 10 years