

CCTV Privacy Impact Assessment – Deployable

Location of surveillance camera system being assessed:
West Suffolk Council CCTV control room

Date of assessment: 2026

Review date: 2027

Name of person responsible: Luke Porter

Level 1 considers the general details of the camera surveillance system and supporting business processes. Level 2 considers the specific implications for the installation and use of cameras.

Level 1

Data Protection Act 2018 and Surveillance Camera Code of Practice

1.	What is the organisation's purpose for using CCTV and what are the issues that the system aims to address?	<ul style="list-style-type: none"> • To assist in the prevention and detection of crime. • To assist in the promotion of community safety and to reduce anti-social behaviour. • To assist the client (system owner) in providing any of its prosecuting or contracted services. • To assist in the management of the town centre – this includes monitoring safety or operationally critical activities on a particular site. • To assist the council in the protection of assets.
2.	Can CCTV technology realistically deliver these benefits?	Since its implementation, CCTV has prevented and deterred crime statistically and it has provided police and courts with the necessary evidence to prosecute anyone engaging in criminal activity.
3.	What are the views of those who will be under surveillance?	<ul style="list-style-type: none"> • CCTV surveillance is supported by the council's endeavour and promise to make the towns which it covers safer and more profitable for its residents and local businesses by preventing and deterring criminal activity. • Assurance is given to members of the public that all our operators are Security Industry Authority (SIA) approved and Non-Police Personnel Vetting (NPPV2) vetted by police and people's rights are covered by the Data Protection Act (DPA) and General Data Protection Regulation (GDPR). • Any future camera requests will require local consultation to comply with the Surveillance Camera Commissioner (SCC) Code of Practice through an approval process, ensuring that new

		<p>installed cameras are installed for their intended purpose only.</p> <ul style="list-style-type: none"> • Deployable cameras have had a large positive response from the public in the area where they are being deployed. There have been multiple surveys and consultations with residents where the public have expressed deployable cameras as the top priority for reducing crime.
4.	Have other less privacy-intrusive solutions, such as improved lighting, been considered?	Other less privacy-intrusive solutions are always considered before the implementation of a new camera. In some cases, improved lighting and CCTV installation co-exist to make a particular area safer for residents.
5.	What are the benefits to be gained from using CCTV?	<ul style="list-style-type: none"> • Public Deployable CCTV helps in the prevention and detection of crime which ultimately leads to criminal prosecution in regard to police/court investigations. • Through its continued success, a town can become a much safer environment for members of the public, but, additionally, attract new businesses to the area allowing a town to economically thrive. • Not only do the operators reactively respond to police airwaves when they have received an emergency call about an incident, but they are also very proactive when monitoring CCTV and it has proven to be highly effective in detection of incidents.
6.	What are the privacy issues arising from this surveillance camera system?	<p>Privacy issues include the following:</p> <ul style="list-style-type: none"> • viewing of private space • recording of personal data • retention and deletion of footage • excessive or inappropriate monitoring.
7.	What privacy design features will be adopted to reduce privacy intrusion?	<p>To ensure privacy, the council has adopted the following features:</p> <ul style="list-style-type: none"> • All cameras have the ability to have masking privacy windows to block operators from viewing inside people's homes or places that are highlighted as private areas. • All operators are SIA trained to understand the DPA and GDPR legislation. • All recorded images are automatically deleted after 31 days. • Evidence handling procedures are in place and updated accordingly. • Management carries out random spot checks on all operators' camera work to ensure there is no excessive or inappropriate monitoring. • Management ensures that all operators are NPPV2 vetted, and training is completed. • System and network configurations are secure and managed by qualified and vetted engineers.

8.	What organisations will be using the CCTV images and who will take legal responsibility for the data under the Data Protection Act 2018?	Data users include: <ul style="list-style-type: none"> • data subjects • statutory prosecuting authorities (police) • clients and authorised investigators.
9.	Do the images need to be able to identify individuals, or could the scheme use other images not capable of identifying individuals?	<ul style="list-style-type: none"> • The CCTV system records images at a high quality and the type and location of cameras and their capabilities will determine whether images of individuals are captured. In most cases our CCTV will capture individuals who are identifiable to help in the prosecution of offenders. • In some cases, we have static cameras that cover a particular site to prevent criminal damage but, in most cases, the pan, tilt, zoom (PTZ) cameras used by us can zoom in and out at a distance and are used proactively to gather identities of individuals involved in criminal activity. • All our PTZ cameras have general pre-set positions which are used to obtain general coverage of an area which minimises personal data capture.
10.	Will the CCTV equipment being installed, and the system of work being adopted, be sustainable? Is there enough funding for the scheme?	<ul style="list-style-type: none"> • The council's CCTV system has a sustainable revenue budget through the charging of services, including that of alarm and CCTV monitoring for other councils and organisations. • Any new cameras or equipment that are installed must have an allocated budget before installation.
11.	Will the system or equipment being considered deliver the desired benefit now and in the future?	<ul style="list-style-type: none"> • The council's CCTV system has been designed for resilience, future compatibility, and expansion purposes. With technology constantly advancing and improving, there will always be a need to upgrade equipment to ensure the CCTV continues to benefit the community. • The deployable cameras being used can be moved/relocated to any area experiencing high levels of crime/ASB.
12.	What future demands may arise for wider use of images and how will these be addressed?	At present, recorded images are only used for public safety and police investigations.

Human Rights Act 1998

1.	Is the system established on a proper legal basis and is it operated in accordance with the law?	The CCTV system was established under section 115 of the Crime and Disorder Act. It operates within the current legislation requirement and is lawfully compliant.
----	--	--

2.	Is the system necessary to address a pressing need, such as public safety, crime prevention or national security?	<ul style="list-style-type: none"> • Like all populated areas, everywhere has its share of crime and disorder, hence it is necessary for CCTV to be installed to achieve public safety and reduce crime. • The council's constant commitment to the prevention and detection of crime resulted in a large investment in the Bury St Edmunds CCTV control room to serve the public in this endeavour to reduce crime in the local areas. • Due to the success of this control room, it has allowed for new cameras to be installed to better provide organisations, including the police, to take evidential footage to court and prosecute against offenders. This success is constantly portrayed in praises and thanks from constabularies and the continued statistics that are held in the control room.
3.	Is it justified in the circumstances?	Public CCTV is justified in that it prevents and deters crime and it has shown to be very beneficial to the council and emergency services which, in turn, is supported by residents and councillors.
4.	Is it proportional to the problem that it is designed to deal with?	It is proportional to the problem it was designed to deal with. This is portrayed in the recent upgrade we undertook on the control room and the room for expansion on all the equipment.
5.	Do any of these measures discriminate against any sections of the community?	The CCTV network used by the council does not discriminate against any sections of the community. All staff are additionally trained, and SIA licensed to ensure that legislation is adhered to.

Level 2

Step 1: Definition of camera types utilised

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.

West Suffolk Council coverage

ID	Camera types	Makes	Description	Justification and expected use
1	Deployable Camera	Hikvision	Re-deployable camera units	Static cameras deployed to target specific areas. PTZ cameras to be deployed in areas experiencing high levels of crime/ASB. All Cameras recorded 24/7 to prevent and detect crime and disorder, as well as ensure public safety and site security.

Step 2: Location assessment

Each system operator or owner should list and categorise the different areas covered by surveillance on their system. This list should use the specifications above, which ID (types) are used at each specific location.

Camera number (Bury St Edmunds)	Location	Camera types used	Total	Recording and monitoring	Assessment of use of equipment (mitigations or justifications)
1, 2, 3, 4, 5, 6, 7, 8, 9, 10,11,12,13,14,15,16,17, 18	Various	1	18	Recorded 24/7 hours a day but only monitored when a report of an incident comes into the control room.	Main purpose of these cameras is to prevent and detect crime for community safety. Deployable cameras are only used in areas where a permanent camera installation cannot be justified or where there is limited wireless coverage.

Highlighted privacy issue

Privacy issue	Risk to individuals	Associated organisation or corporate risk	Solution	Evaluation
Collecting and exceeding purposes of CCTV system	New surveillance methods may be unjustified intrusion on person's privacy.	<ul style="list-style-type: none"> Loss of reputation Fines and sanctions 	Update technology to ensure that the collection of information and images does not exceed the primary functions of the service.	Privacy zones should be activated where a camera may intrude upon an individual's private residence. All data collected must, always, be justified, compliant and proportionate.
Retention of images and information for longer than necessary	Retaining personal images and information longer than necessary will breach people's personal data.	<ul style="list-style-type: none"> Loss of reputation Fines and sanctions 	Only allow recording of images and footage to be held for 31 days. Dispose of all other information that is not relevant to criminal investigation.	Retention of 31 days on all servers in place. Anything past the 31 days will be destroyed.
Lack of policies and procedures and mechanisms	No public availability of CCTV code of practice which details how personal data will be handled, stored and disclosed.	<ul style="list-style-type: none"> Loss of reputation Fines and sanctions 	Produce a code of practice and publish this on the website to increase transparency.	Code of practice in place and published for transparency.
Signage	Public not made aware that they are entering an area which is monitored by a CCTV system.	<ul style="list-style-type: none"> Loss of reputation Fines and sanctions 	Survey analysis to take place.	Survey conducted to highlight areas where there is not enough signage. Signage to be installed where it is lacking as a priority.

Privacy issue	Risk to individuals	Associated organisation or corporate risk	Solution	Evaluation
Re-deployable cameras	Public not made aware that they are entering an area which is monitored by a CCTV system.	<ul style="list-style-type: none"> • Loss of reputation • Fines and sanctions 	Install signage in immediate area to inform public they are entering a CCTV monitored area.	Survey of area to be conducted for all re-deployable sites.

Level 3

1. How is information collected?

- CCTV camera
- Body worn video (BWV)
- Automatic number plate recognition (ANPR)
- Unmanned aerial systems (drones)
- Stand-alone cameras
- Real time monitoring
- Other (please specify):

2. Does the system's technology enable recording?

- Yes No

Please state where the recording will be undertaken (no need to stipulate address, just local authority CCTV control room or on-site would suffice for stand-alone camera or BWV), and whether it also enables audio recording.

Recording takes place on sites owned by West Suffolk Council.

3. Is the recording and associated equipment secure and restricted to authorised person(s) (please specify – for example, in secure control room, access restricted to authorised personnel)?

Access to recordings is kept secure on our managed network and access to footage can only be done through the control room.

4. What type of transmission is used for the installation subject of this PIA (tick multiple options if necessary)?

- Fibre optic
- Wireless
- Hard wired
- Broadband
- Other (please specify): 4G Sim Card

5. What security features are there to protect transmission data – for example, encryption (please specify)?

All cameras and footage are on a secure network with encryption.

6. Where will the information be collected from?

- Public places
- Car parks
- Buildings and premises (external)
- Buildings and premises (internal public areas)

7. From whom or what is the information collected?

- General public in monitored areas (general observation)
- Vehicles
- Target individuals or activities (suspicious persons or incidents)
- Visitors
- Other (please specify):

8. What measures are in place to mitigate the risk of cyber-attacks which interrupt service or lead to the unauthorised disclosure of images and information?

Patching of our systems is conducted on a monthly basis to minimise the risk of cyber attack.
Our network is also managed by our internal IT team and our systems are additionally penetration (PEN) tested on an annual basis.

9. How is the information used (tick multiple options if necessary)?

- Monitored in real time to detect and respond to unlawful activities
- Monitored in real time to track suspicious persons or activity
- Compared with reference data of persons of interest through automatic facial recognition software
- Compared with reference data for vehicles of interest through automatic number plate recognition software
- Used to search for vulnerable persons
- Used to search for wanted persons
- Recorded data disclosed to authorised agencies to support post incident investigation, including by law enforcement agencies
- Recorded data disclosed to authorised agencies to provide intelligence
- Other (please specify):

10. How long is footage stored (please state retention period)?

31 days unless requested to be downloaded for an ongoing police investigation.

11. Retention procedure

- Footage automatically deleted after retention period
- System operator required to initiate deletion
- Under certain circumstances, authorised persons may override the retention period – for example, retained for prosecution agency (please explain your procedure)

If footage is required for evidential purposes in a police investigation, then footage can be downloaded upon receiving a download request form.

12. With which external agencies and bodies is the information and footage shared?

- Statutory prosecution agencies
- Local government agencies
- Judicial system
- Legal representatives
- Data subjects
- Other (please specify):

13. How is the information disclosed to the authorised agencies?

- Only by onsite visiting
- Copies of the footage released to those mentioned above (please specify below how released – for example, sent by post or courier): Encrypted cloud
- Offsite from remote server
- Other (please specify):

14. Is there a written policy specifying the following (tick multiple boxes if applicable)?

- Which agencies are granted access
- How information is disclosed
- How information is handled
- Recipients of information become data controllers of the copy disclosed

15. Are these procedures made public?

Yes No

16. Are there auditing mechanisms?

Yes No

If so, please specify what is audited – for example, disclosure, production, accessed, handled, received or stored information)

Our current system audits everything in regard to stored information.

17. Do operating staff receive appropriate training to include the following?

- Legislation issues
- Monitoring, handling, disclosing, storing, deleting information
- Disciplinary procedures
- Incident procedures
- Limits on system uses
- Other (please specify):

18. Do CCTV operators receive ongoing training?

Yes No

19. Are there appropriate signs which inform the public when they are in an area covered by surveillance camera systems?

Yes No

All cameras will be reviewed on an annual basis and any new additions to our system will be added.

The PIA process

The diagram below shows the six stages of the PIA process.

The PIA process

