SAFE WELL PROSPEROUS CONNECTED

Information Governance Framework

Schedule 03D

CCTV Policy

North Lincolnshire Council

www.northlincs.gov.uk

Background Information	
Document Purpose and Subject	To provide a council-wide policy for CCTV
Author	Information Governance Team.
Document Owner	Information Governance Team.
Change History	V1.7 - The policy has been updated to take into account new guidance from the Information Commissioner on CCTV and Video Surveillance, at section 1.0 to explain personal data in the context of video surveillance and to list further applicable legislation, at section 2.0 to update the scope of the policy and to explain about common types of surveillance included in the ICO guidance, at section 3.0 to update the legislation list, at section 6.0 to update in line with the ICO guidance, at section 8.0 to include a sentence on the recording of audio, at section 9.0 to include information about linking data and to update the requirement to carry out a DPIA before implementing and changing surveillance systems and Appendix A has been updated at point c) to include that at times the council works in partnership with the police and will share video surveillance under the Crime and Disorder Act 1998.
File Location	Information Governance Shared Storage Area
Retention Period	Permanent Preservation as a Core Policy.
Issue Date	28 November 2022
Last Review	January 2022
Current Review	November 2022
Next Review Date	March 2023
Approved By	Cabinet Member
Approval Date	23 November 2022

Contents

1. Introduction

Video surveillance systems are used by North Lincolnshire Council in areas including those in and around the town centre, in some council buildings, at recycling centres, in areas where there is for example a problem with fly tipping, as body worn cameras on community wardens and on refuse collection vehicles. It is used as a valuable tool to assist with public safety and security and to protect property.

Video surveillance systems owned and maintained by North Lincolnshire Council and are operated to the requirements of the UK General Data Protection Regulation and good practice guidelines, such as those issued by the Information Commissioner's Office (ICO) in the Video Surveillance Code of Practice, to ensure for example that the need for public protection is balanced with respect for the privacy of individuals.

The UK GDPR applies because video surveillance systems capture personal information that could identify someone. This policy outlines the principles we adhere to, the processes that we follow and related policies and processes, such as those about how to request information including CCTV images. Each video surveillance system will also have a Code of Practice to set out the intended purpose and to provide further detail.

The UK GDPR defines personal data as any information relating to an identified or identifiable natural person who can be identified directly or indirectly in particular by reference to an identifier such as name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Biometric data is defined as personal data resulting from specific technical processing relating to physical, physio-logical or behavioural characteristics or a natural person, which all or confirm the unique identification of that person, such as facial images or fingerprint data.

The aim of this policy is to set out a consistent approach for the use of video surveillance by North Lincolnshire Council and it covers:

- How and why video surveillance is used;
- Compliance with legislation, such as the:
    - UK General Data Protection Regulation (UK GDPR) / Data Protection Act 2018 (DPA);
    - Freedom of Information Act;
    - Human Rights Act;
    - Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012

- The requirement for each operator (Manager) of a video surveillance system to put in place a Code of Practice for use.
- The requirement for each operator (Manager) of a video surveillance system to provide annual assurance of compliance with this policy and the specific CCTV Code of Practice.
- The requirement for new major video surveillance systems or major changes to existing ones to be approved by the responsible Director and responsible Cabinet Member and for minor changes or installations to be approved by the Service Manager as a minimum. A major change could be the introduction of a different type of surveillance equipment or the installation of a significant number of new cameras to an existing scheme. A minor change could be the installation of new scheme within a council building or the addition of one or two cameras to an existing scheme.

This policy is part of a suite of Information Governance policies and procedures.

2. Scope

This policy applies to all overt (open) video surveillance systems controlled by the council. This includes both internal and external video surveillance cameras, fixed and mobile traditional CCTV cameras, automated number plate recognition (ANPR) cameras, Body Worn Video (BWV), Drones (UAVs), Facial Recognition Technology (FRT) and Dashcams. This policy applies to all council employees and all individuals or organisations acting on behalf of the council. Any other organisation operating a surveillance system in a council building and schools who are Data Controllers in their own right operating a system within the school can adopt this policy or is expected to have their own comparable policy.

The Protection of Freedoms Act states that 'surveillance camera systems' means:

a) Closed Circuit television or automatic number plate recognition systems.
b) Any other systems for recording or viewing visual images for surveillance purposes.
c) Any systems for storing, receiving, transmitting, processing, or checking images for information obtained by systems falling within a) or b).
d) Any other systems associated with, or otherwise connected with, systems falling within a), b) or c).

<u>This policy applies to surveillance systems including</u>:

1) Traditional CCTV systems.

   Traditional CCTV systems can be either fixed for mobile and tend to be used to capture and store images.

2) Automatic Number Plate Recognition (ANPR):

ANPR systems can collect and analyse large quantities of data and capture images as vehicles drive past their field of vision. ANPR systems generally capture images of vehicles, the vehicle number plate (plate patch) and the vehicle registration mark (VRM). Number plates can then in some instances be cross referenced with live UK databases.

In most cases the VRM is personal data such as when using it to identify someone, but this depends on the context of the processing.

3) Body Worn Video (BWV):

BWV involves the use of cameras that are worn by a persona and are often attached to the front of clothing. The cameras record by footage and audio and generally only record when switched on with the intention of recording.

4) Unmanned Aerial Vehicles or Drones (UAVs):

Drones or UVAs are lightweight unmanned aircraft commonly controlled by operators. They are used for reasons including photography and the taking of videos. Care is required to ensure personal data is not collected, used for shared about individuals who were not the intended focus of the recording and who are unlikely to have realised they were recorded.

Council operated drones will be registered in compliance with the requirements set out on the Civil Aviation Authority (CAA) Drone Safe Website.

5) Facial Recognition Technology (FRT):

FRT identifies or otherwise recognises a person from a digital facial image. Cameras are used to capture images and facial recognition software measures and analyses facial features. Biometric data is generally captured and other personal data depending on the reason for use.

6) Dashcam Surveillance in Vehicles:

Surveillance systems in vehicles can have inward or outward facing cameras used to record footage of the journey and any incidents. Generally, dashcams can record images and audio, but audio will only be recorded in council owned vehicles where this can be justified.

7) Workplace Surveillance and Live Streaming:

Surveillance in the workplace is generally used for the health and safety, and for the security of employees. Prior to the introduction of such a system employees will be consulted, clear notices will be displayed, surveillance will be targeted in areas of particular risk where expectations of privacy are low,

continuous monitoring and/or audio recording will only be used where justified, and employees will be made aware of how to raise concerns.

Day to day monitoring can involve the footage being retained for an agreed length of time or by live streaming where no data is saved but the footage can be viewed in real time. The most appropriate method of monitoring is considered.

The use of video conferencing at an online meeting will be explained at the start of the meeting including any choice or control over the recording and if and how it will be communicated to attendees.

8) Any other surveillance system that has the potential to process personal data:

At times electronic devices such as mobile phones or tablets may be used to capture images, because they provide a versatile method of filming that traditional CCTV cameras are not suitable for. Where images from these devices are sent to the council or where these devices are used by council to capture images the processing of the images will have the same level of security and governance to that provided by other surveillance technologies and will respect the rights and freedoms of individuals.

This policy does not apply to the covert (secret) use of CCTV cameras that is covered by the council's Regulation of Investigatory Powers (RIPA) Policy.

3. Associated Legislation

Video surveillance systems owned and operated by North Lincolnshire Council comply with the following legislation so that they are lawful, fair, and transparent:

- UK General Data Protection Regulation / Data Protection Act 2018;
- The Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012 (PoFA)
- Crime and Disorder Act 1998;
- Human Rights Act 1998;
- Protection of Freedoms Act 2012;
- Freedom of Information Act 2000;
- Regulatory and Investigatory Powers Act 2000.

4. Associated Processes and Documentation

Associated process documents and forms are in place to aid compliance with the CCTV Policy, as follows:

- Subject Access request form – IG24
- Data Protection Act 2018 Schedule 2 request form – IG25

5. Surveillance Camera Commissioner

The Secretary of State has issued a Surveillance Camera Code of Practice under section 30 of the Protection of Freedoms Act 2012, which provides guidance on the use of surveillance systems. It explains how the government is supportive of the use of overt surveillance provided that certain conditions are met. Compliance is achieved by fulfilling twelve guiding principles that we have adopted, as shown below:

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 securely 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.

The Surveillance Camera Commissioner is a statutory appointment by the Home Secretary to promote compliance with the Surveillance Camera Code of Practice and to provide advice on compliance. A Surveillance Camera Commissioner CCTV Guide, a Passport to Compliance document, Self-Assessment Tools and Data Protection Impact Assessments templates for Surveillance Cameras have also been created by the Secretary of State to assist organisations with compliance. The Commissioner has no enforcement or inspection powers.

6. Information Commissioner's Video Surveillance Code of Practice

The ICO has produced a Video Surveillance Code of Practice in 2022 to assist organisations who use video surveillance to comply with legislation and good practice. The aim of the ICO guidance is to:

- Help to ensure the use of personal information connected to video surveillance is lawful and complies with the UK General Data Protection Regulation and the Data Protection Act 2018.
- Contribute to the efficient deployment and operation of surveillance systems.
- Mean that personal data processed is usable and that processing meets intended objectives.
- Reassure those whose personal data is being processed.
- Help inspire wider public trust and confidence in the use of surveillance systems.
- Reduce reputational risks by staying within the law and avoiding regulatory action and penalties.

7. Information Commissioner's Employment Practices Code

Where employees could be monitored in the workplace Section 3 of the Information Commissioner's Employment Practices Code will be taken into account to assist

with compliance with Data Protection legislation and Article 8 of the Human Rights Act.

8. Why is Video Surveillance used and how?

The purpose of the video surveillance system must be identified and documented, and the reasons why surveillance is the most appropriate means of meeting the scheme aims and whether these can be met in another less intrusive way.

We are using video surveillance for the following purposes:

1) Public and employee safety.
2) Employee conduct.
3) To increase property security.
4) To increase vehicle security.
5) To reassure individuals and reduce the fear of crime.
6) For the prevention, investigation and/or detection of crime.
7) Apprehension and/or prosecution of offenders.

Each surveillance system will have a Code of Practice, produced by the responsible manager and which provides more detailed information so that everyone is aware of the purpose for the scheme and how it should be operated.

Video surveillance systems will be operated fairly, within applicable law and only for the purposes for which they were established, or which are subsequently agreed in accordance with this Policy. Schemes will be operated with due regard to the privacy of the individual.

Video surveillance cameras within the council's Security Control Centre a monitored 24 hours per day, 365 days per year by council staff who work in partnership with the Police who can view the images under the Crime and Disorder Act 1998.

Audio recording is considered more intrusive than the recording of images and it will only be used where it has been justified.

9. Installation and Operation of Video Surveillance

Prior to the installation of video surveillance systems and extensions to existing schemes where necessary consultation will take place with the police and any other interested parties.

With the exception of Body Worn Cameras council CCTV schemes do not record sound or if this functionality is available, it will be disabled.

Video surveillance systems will be able to produce images of sufficient quality for the purpose. No dummy cameras will be used in any scheme.

This policy and the locations of CCTV cameras monitored by the council's Control Centre will the published on our website.

Video surveillance will not be hidden and signs to show that video surveillance is operating will be displayed at the perimeter of the areas covered by the scheme and at other key points. The signs will be:

1) Be clearly visible and readable;
2) Contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact about the scheme (where these things are not obvious to those being monitored);
3) Include basic contact details such as a simple website address, telephone number or email contact; and
4) Be an appropriate size depending on context. For example, whether they are viewed by pedestrians or car drivers.

This is to inform the public that video surveillance is in operation, who is operating the scheme and how to contact them and to allow those entering the area to make a reasonable approximation of the area covered by the scheme.

Operators of video surveillance systems and associated equipment will act with the utmost integrity and only employees with responsibility for using the equipment will have access to operating controls.

Surveillance technologies can be interconnected so that information can the shared or linked, and in some cases integrated into a broader 'big data' system. Where information is used in this way care will be taken to ensure accuracy, that the data used is not excessive, that the data is only used for a defined purpose and that the use of data in this way is necessary and proportionate. The ICO guidance on big data will be followed where relevant.

A Data Protection Impact Assessment (DPIA) will be carried out on new systems and extensions to existing ones where the surveillance is likely to result in a high risk to individuals, including where special category data will be processed, where there is monitoring of a publicly accessible place on a large scale or where individuals are monitored in the workplace. This ensures all privacy matters have been considered and any risks removed or reduced to an acceptable level. The Data Protection and Confidentiality Policy provides further information about the DPIA process.

10. Location of Video Surveillance

The location of video surveillance equipment is important and must be carefully considered. The areas to be covered must be clearly identified, and the way in

which images are recorded must comply with UK GDPR Data Protection Principles as follows:

- Video surveillance must only monitor those spaces intended to be covered.
- Video surveillance must be sited to ensure that it complies with purpose of the scheme.
- If there is a risk of neighbouring area being monitored the owner of the area must be consulted.
- Adjustable surveillance equipment must be operated to prevent unintended areas being monitored.
- Some areas have heightened expectations of privacy, such as changing rooms and toilets. Video surveillance must only be used in most exceptional circumstances to address very serious concerns.

11. Complaints and Security Incidents

We aim to provide efficient and effective services. If individuals feel that a council video surveillance installation is not being operated as set out in this Policy or a related Code of Practice, or that their request for access to personal data captured by a video surveillance system has not been dealt with in a satisfactory manner they can complain, and a review will be carried out using the council's Information Complaints Policy.

Appendix A – Requesting Video Surveillance Images

Everyone has the right to request video surveillance image information under either the UK General Data Protection Regulation (GDPR) / Data Protection Act 2018 or the Freedom of Information Act 2000 (FOIA). Details of how to make a request can be found in our Access to Information Policy, published in the Information Governance area of the website, and requests will be considered on a case-by-case basis.

a) UK GDPR Subject Access Requests

The UK GDPR provides individuals with the right to request video surveillance images that contain their personal information by making a Subject Access Request (SAR).

b) DPA 2018 Schedule 2 Requests

Schedule 2 of the Data Protection Act 2018 provides an exemption that allows organisations that have a crime prevention, law enforcement or tax collection function to request video surveillance images containing personal information to prevent or detect a crime, apprehend, or prosecute an offender, or for taxation / benefit purposes. Examples are the Police, HM Revenue and Customs, the Health and Safety Executive and Solicitors.

There is also an exemption under Schedule 2 that allows requests for video surveillance images in connection with legal proceedings, or where disclosure of video surveillance footage is required by law.

In some cases, there may be a charge to obtain copies of the requested footage, although there will be no charge to review images under supervision where this is appropriate and no charge for us to review images on your behalf.

c) Crime and Disorder Act 1998

There are times when the council works in partnership with the Police and will share video surveillance information under the Crime and Disorder Act 1998.

d) Freedom of Information Requests

Generally, video surveillance images will be exempt from release under the Freedom of Information Act if someone could be identified from the image. However, questions about the operating of a video surveillance system may be received and it may be appropriate to answer these questions under this Act.

e) Internal Requests for Information

Sometimes council managers will need to request access to video surveillance images in connection with internal investigations. These requests should be made in writing to the responsible manager of the video surveillance Scheme and will be considered in line with Data Protection legislation that includes discussion with the council's Data Protection Officer.