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	V1.5 - The policy has been updated to make reference to the UK GDPR, applicable from 01 January 2021. The policy has also been updated in section 1.0 to amend the approval for new cameras and schemes, at section 3.0 to include the Crime and Disorder Act 1998, at Section 8.0 to explain that the Police view Security Control Centre images under the Crime and Disorder Act 1998, at section 9.0 to state that Body Worn Cameras have sound recording and in Appendix A to say that internal requests to view CCTV images should be discussed with the Data Protection Officer
File Location	Information Governance Shared Storage Area
Retention Period	Permanent Preservation as a Core Policy.
Issue Date	31 March 2021
Last Review	January 2020
Current Review	January 2021
Next Review Date	March 2022
Approved By	Cabinet Member
Approval Date	23 March 2021

Contents

1. Introduction

Closed Circuit (CCTV) is used by North Lincolnshire Council in areas including those in and around the town centre, in some council buildings, at recycling centres, 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.

The CCTV installations are 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), to ensure for example that the need for public protection is balanced with respect for the privacy of individuals.

The UK GDPR applies because CCTV cameras 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 CCTV installation will also have a Code of Practice to set out the intended purpose and to provide further detail.

The aim of this policy is to set out a consistent approach for the use of CCTV Surveillance and it covers:

- How and why CCTV Surveillance is used;
- Compliance with legislation, such as the UK General Data Protection Regulation (UK GDPR) / Data Protection Act 2018 (DPA);
- The requirement for each operator (Manager) of a CCTV installation to put in place a Code of Practice for use.
- The requirement for each operator (Manager) of a CCTV installation to provide annual assurance of compliance with this policy and the specific CCTV Code of Practice.
- The requirement for new major CCTV installations 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 recording 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) CCTV installations controlled by the council. This includes both internal and external cameras, fixed and mobile cameras, automated number plate recognition (ANPR) cameras and Body Worn Recording cameras. This policy applies to all council employees and all individuals or organisations acting on behalf of the council.

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.

Schools, who are Data Controllers in their own right, may choose to adopt this policy but where this is not the case it is expected that they will have their own appropriate policy.

3. Associated Legislation

Any CCTV Scheme owned and operated by North Lincolnshire Council must comply with the following legislation:

- UK General Data Protection Regulation / Data Protection Act 2018;
- 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 CCTV cameras. It explains how the government is supportive of the use of overt CCTV 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 CCTV Code of Practice

The ICO has produced a Data Protection Code of Practice for Surveillance Cameras and Personal Information (Revised edition 2017 - version 1.2) to assist organisations who use CCTV to comply with the General Data Protection Regulation / Data Protection Act 2018.

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 CCTV used and how

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

We are using CCTV 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 CCTV scheme 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.

CCTV schemes 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.

CCTV 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 are able to view the images under the Crime and Disorder Act 1998.

9. Installation and Operation of Cameras

Prior to the installation of CCTV schemes 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.

Cameras 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 will the published on our website.

Cameras will not be hidden and signs to show that CCTV cameras are 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 cameras are 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 cameras and associated equipment will act with the utmost integrity and only employees with responsibility for using the equipment will have access to operating controls.

A Data Protection Impact Assessment (DPIA) will be carried out on all CCTV installations and extensions to schemes, to ensure all privacy matters have been considered and any risks either removed or reduced to an acceptable level. The

Data Protection and Confidentiality Policy provides further information about the DPIA process.

10. Location of Cameras

The location of the CCTV 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 Data Protection Principles as follows:

- Cameras must only monitor those spaces intended to be covered.
- Cameras must be sited to ensure that they comply with purpose of the scheme.
- If there is a risk of neighbouring area being monitored the owner of the area must be consulted.
- Adjustable cameras must be operated to prevent unintended areas being monitored.
- Some areas have heightened expectations of privacy, such as changing rooms and toilets, and cameras 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 CCTV installation is not being operated as set out in this Policy or a related Code of Practice, or that their request for access to a CCTV image 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 CCTV Images

Everyone has the right to request CCTV 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) GDPR Subject Access Requests

The GDPR provides individuals with the right to request CCTV 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 can request CCTV 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 CCTV images in connection with legal proceedings, or where disclosure of CCTV footage is required by law.

d) Freedom of Information Requests

Generally CCTV 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 the CCTV 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 CCTV images in connection with internal investigations. These requests should be made in writing to the responsible manager of the CCTV Scheme and will be considered in line with Data Protection legislation that includes discussion with the council's Data Protection Officer.