Copeland borough council

Proud of our past. Energised for our future.

Surveillance Equipment Policy

Version: V1.2
Policy Date: October 2022

Document Control

Organisation	Copeland Borough Council
Title	Surveillance Equipment Policy
Version	V1.2
Author	Surveillance Equipment Working Group
Filename	Surveillance Equipment Policy
Owner	Data Protection Officer
Subject	Surveillance Equipment
Protective Marking	
Review Date	January 2023

Note: This document is uncontrolled if printed or reproduced

Revision History

Version Reviewed	Date Reviewed	Reviewed By	Description of Revision
V1.0	November 2019	CBC Surveillance Camera Code of Practice Working Group	Draft
V1.0	October 2021	Director Corporate Services and Commercial Strategy, Property & Estates Manager, Information Governance & Data Compliance Officer, Policy Officer	Update and refresh of 2019 draft.
V1.1	October 2022	Information Governance and Data Compliance Officer	Additional CCTV systems added.

Document Approval

Version	Approved By	Date
V1.1	**Corporate Leadership Team**	20.10.2021
	Trade Union Consultation	
	Overview & Scrutiny	04.11.2021
	Executive	
	Full Council	07.12.2021

Document Distribution

This policy is to be available to all staff and elected members of Copeland Borough Council and placed on the Council's intranet site and external website. A copy must also be provided to contractors and third parties undertaking work on Copeland Borough Council premises.

Contributors

Surveillance Camera Commissioner	Code of Practice
Barrow Borough Council	Closed Circuit Television Protocol
South Lakeland District Council	CCTV Policy
CBC Surveillance Camera Code of Practice Working Group	

Contents

Purpose

Section 33 of the Protection of Freedoms Act 2012 requires all local authorities to pay due regard to the Surveillance Camera Code of Practice (SCCoP) where they operate surveillance cameras overtly in public places. All surveillance camera systems will be processing personal data so must comply with both the Data Protection Act 2018 and the requirements under General Data Protection Regulation (GDPR).

Copeland Borough Council (CBC) currently has Closed Circuit Television (CCTV) at the following locations:

- Market Hall
- Moresby Depot
- Distington Crematorium
- The Beacon
- The Copeland Centre
- Leconfield Industrial Estate
- Castle Park
- 360 degree CCTV – operational vehicles

The SCCoP also covers other surveillance devices such as body-worn cameras, automatic number plate recognition systems, mobile phone cameras, etc.

This Policy explains how Copeland Borough Council will manage and operate surveillance equipment systems under their control.

Where CBC tenants have surveillance systems that impacts on areas outside of their occupation in the ownership of the Council, CBC will endeavour to ensure their policies and procedures align with this policy.

The aim of the policy is to provide clear information on how we will use the CCTV system and to provide a framework for the use, retention and viewing of the CCTV images and to ensure that CBC meets the requirements of legislation including:

- Surveillance Camera Code of Practice
- General Data Protection Regulation
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000.
- Data Protection Act 2018

Policy Benefits

This policy enables CBC to comply with the twelve guiding principles of the Surveillance Camera Code of Practice:

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 it 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 image 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, 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.

Introduction

Purpose

The purpose of installing surveillance equipment systems is to:

- Reduce crime and assist the prevention of crime.
- Reduce the fear of crime and promote community safety.
- Protect council property.
- Provide evidence which may be used to prosecute offenders.
- Ensure the safety of visitors and staff using council property.
- Meet insurance requirements. For example, indemnity policies for specific exhibition loans to the Beacon Museum.
- Provide an efficient and effective service at the crematorium.
- Assist in evidence gathering for internal CBC investigations. For example, misconduct or health and safety incidents.
- Purposes in accordance with guiding principle 11 above where not captured in the preceding purposes.

Operation

CCTV cameras will be fixed to focus on specific areas of council property.
The cameras do not have sound recording capability.
The camera at the entrance to the Leconfield Industrial Estate has Automatic Number Plate Recognition capability (ANPR).
The cameras will not be used for covert surveillance unless authorisation is granted under the Regulation of Investigatory Powers Act.

Surveillance Equipment Signs

Clear signage will be displayed to advise staff and building users and members of the public that CCTV is in operation.

Data Subject Rights

Any application to access images should be made to Corporate Governance Team in writing via e mail to: freedomofinformation@copeland.gov.uk

An individual has the right to be informed of the following:

- Whether any personal data involving the individual has been processed.
- If so, a description of the personal data.
- The purpose for which it was processed
- Those parties to whom the data can be disclosed

CBC Privacy notice can be accessed on our Website and using the following link:
Privacy Notice | Copeland Borough Council

Surveillance Equipment Control

Standard operating procedures for each system are to be established for each system by the system owner based on this policy and the SCCoP.
There will be restricted viewing and disclosure of images obtained via surveillance equipment as permitted by the Responsible Officer (Information Governance and Data Compliance Officer) and Authorised Operational Staff at each of the locations where Council controlled surveillance equipment is installed. In the absence of the Responsible Officer (Information Governance and Data Compliance Officer), the Senior Information Risk Owner (SIRO) will oversee any requests.

Images will only be accessed if the purposes listed at page 7 are apparent. Access will only be permitted when authorised and may require the use of a RIPA authorisation. In this case the Responsible Officer will work with the SIRO.

In any event, an incident log will be recorded giving a reason for the request and access to images. (Appendix A)

Scope

Storage of images

Images collected via surveillance equipment will routinely be stored for a specified period of time, after which they will be automatically overwritten or deleted.

On occasion, there may be a need to retain images for a longer period. For example, if an incident is identified as per 'purpose' at page 7, or where a law enforcement body is investigating a crime and asks for it to be preserved to give them opportunity to view the information as part of an active investigation. The extended length of time the images are stored will vary on a case-by-case basis. Once the image is no longer required the same will be deleted/overwritten within 14 days of the Council being informed by investigating authority.

The images will routinely be stored on the individual CCTV system hard drives, unless copies are required by investigating authorities (see below).

Release of images to the police

If the incident is reported to the police the Council may provide the police with copies of the CCTV footage to support detection or solving of crimes. Trawling of images will not be permitted. A crime, incident number or proof that there is an ongoing investigation must be provided.

The Police have a lawful basis for request of disclosure of personal data from organisations. Disclosure is covered under the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

Requests for disclosure will be made using agreed procedures by way of a Data sharing Request made by the Police to CBC.

There may be instances where CBC are unable to release images, however, will work with the Police to ensure images can be viewed under CBC supervision.

Release of images to the media

Images will not be released to the media unless requested by the police to assist in the detection of a crime and will require the agreement of the Responsible Officer (Information Governance and Data Compliance Officer), and in their absence, the Senior Information Risk Owner (SIRO).

Complaints

Complaints about the use and operation of surveillance equipment used by the Council can be made using the Council's Complaints procedure, which is published on the website.
Contact us | Copeland Borough Council

Definitions

Surveillance equipment

The only surveillance equipment used by Copeland Borough Council is Closed Circuit Television.

Roles and Responsibilities

The management of images collected via surveillance equipment is the responsibility of the Authorised Operational Staff for which it is installed with the oversight from the Responsible Officer (Information Governance and Data Compliance Officer), and in their absence, the Senior Information Risk Owner (SIRO).

If an incident is identified as per 'purpose' at page 7 or a request is made by a law enforcement agency the Responsible Officer may extend the storage period of images. This must be documented stating the purpose and proposed length of the extended storage period.

The CCTV system can be intrusive to people carrying out lawful activities and due consideration needs to be given to the justification for installing systems. In each case CBC has undertaken a review of their CCTV installations, the requirement for which has been authorised by the SIRO.

New surveillance systems

Data Protection Impact Assessments

The Council requires all its services to carry out Data Protection Impact Assessments (DPIAs) when they introduce new technology or changes to the processing of personal data. The assessment identifies the risk to privacy from the customer's perspective and what steps can be taken to reduce this wherever possible whilst providing a service to the customer. The information owner of the new technology or process should carry out the DPIA with the guidance of the Corporate Governance Team.

Monitoring of Policy Adherence

All staff using or monitoring surveillance equipment will be made aware of the requirements of this policy and related procedures.

The policy will be reviewed on an annual basis to ensure compliance with relevant legislation and guidance.

References

General Data Protection Regulation
Human Rights Act 1998
Regulation of Investigatory Powers 2000
Freedom of Information Act 2000
Data Protection Act 2018
Surveillance Camera Code of Practice
CBC Data Protection and GDPR Policy
CBC Records Retention Policy

Appendix A

Surveillance Equipment Incident Log	
Date of request	
Briefing:	[insert details – circumstances and reasons for access to images]
Requesting Officer:	
Subject Access Request	Yes/No
Authorisation Given:	Yes/No
Authorising Officer(s):	
Date:	

All requests must be made to the Responsible Officer (Information Governance and Data Compliance Officer) and Authorised Operational Staff at each of the locations where Council controlled surveillance equipment is installed. In the absence of the Responsible Officer (Information Governance and Data Compliance Officer), the Senior Information Risk Owner (SIRO) will oversee any requests.