Mid Devon District Council

Surveillance and CCTV Policy

Policy Number: HSG

November 2024

Version Control Sheet

Title: **Surveillance and CCTV Policy**

Purpose: **To ensure the principles, purposes, operation and management adopted by the main public-space CCTV system are mirrored across the whole of MDDC's service delivery operational areas.**

Owner: **Head of Finance, Property & Climate Resilience**

Pdeal@middevon.gov.uk

Telephone number: 01884 234254

Date: **November 2024**

Version Number: ***2*.0**

Status: **Draft**

Review Frequency: **Every 3 years or sooner if required and in accordance with legislation**

Next review date: **November 2027**

Consultation **This document was sent out for consultation to the following:**

- Group Managers:
- Cabinet Member
- Property Services
- Legal Services
- Information Management

Document History

This document obtained the following approvals.

Title	Date	Version Approved
Corporate Management Team	15 November 2024	2.0
Leadership Team	19 November 2024	2.0
Community PDG	3 December 2024	2.0
Cabinet	10 December 2024	2.0
Council		

1. Definitions and Abbreviations

Body Worn Video cameras (BWV): small, visible camera devices worn attached to an MDDC officer's clothing (usually on the chest). They are used to capture both video and audio evidence when officers are attending incidents and/or carrying out MDDC business.

CCTV Control Room (CR): A secure space located within Tiverton where connected CCTV and surveillance equipment systems are managed and operated in the day to day management of public areas.

Data Protection Act 2018: The legislation that enacts and amends Regulation (EU) 2016/679 (GDPR) and Directive (EU) 2016/680 (Law Enforcement Directive) respectively.

ECHR: European Convention on Human Rights

UK General Data Protection Regulation (UK GDPR): A Regulation establishing data protection principles and privacy rights for people whose data is processed in the European Union.

Information Governance: The discipline of applying controls to how information or data is created, how it is stored and where it moves.

Monitoring Officer: A statutory role under section 5 of the Local Government and Housing Act 1989 whose role is to ensure that the Council, its officers and elected members maintain the highest standards of conduct which includes ensuring the lawfulness and fairness of decision making.

Responsible Officer (RO): A Responsible Officer (RO) is appointed at all sites or business areas using surveillance systems. They are responsible for the day-to-day management of the CCTV system. The RO should support the SPOC in understanding any changes to their system, whether the system remains fit for purpose and whether a maintenance contract is still in place for the system.

RIPA: The Regulation of Investigatory Powers Act 2000. This Act sets out the conditions under which investigations and covert surveillance can be lawfully conducted.

Senior Information Officer (SIO) (as acting Data Protection Officer (DPO)): A statutory role set out under the Data Protection Act with responsibility for ensuring that organisations are compliant with personal privacy rights. Any resident can report a personal privacy concern about the Council to the SIO.

Senior Responsible Officer (SRO): The SRO is the Director of Legal, People & Governance (Monitoring Officer) and has strategic responsibility for compliance with the Protection of Freedoms Act 2012 (PoFA) in support of the Chief Executive in respect of all relevant surveillance camera systems operated by MDDC.

Single Point of Contact (SPOC): The role is operational in support of the SRO and DPO for all matters relating to surveillance systems. The SPOC will act as the main contact point for anything related to a surveillance camera system and apply consistent policies and procedures to all systems at an operational level.

Surveillance Camera Systems (SCS):

SCS has the meaning given by Section 29(6) of Protection of Freedoms Act 2012 and includes:

1. closed circuit television (CCTV) or automatic number plate recognition (ANPR) systems
2. any other systems for recording or viewing visual images for surveillance purposes
3. any systems for storing, receiving, transmitting, processing or checking the images or information obtained by 1 or 2
4. any other systems associated with, or otherwise connected with 1, 2 or 3

This excludes any camera system used for the enforcement of speeding offences.

2 Introduction

2.1 This policy governs the operation of SCS operated by Mid Devon District Council (MDDC) as data controller to assist in its carrying out its enforcement, public safety and other functions.

2.2 The policy sets out the principles to be observed by MDDC, Members, officers, contractors, and any other parties or organisations involved in the operation, management and administration of relevant SCS, as well as the hierarchy of responsibilities which exist to ensure that these systems are operated in a compliant manner.

2.3 It is also intended to inform members of the public of the purposes for which SCS are operated, and of the standards which will be met in relation to it. In this way, MDDC can be held accountable for its compliance with the policy.

2.4 The policy is supplemental to any safe operating procedures for Council departments to follow when procuring and installing SCS.

2.5 This policy does not govern MDDC's use of the surveillance powers available to it, which are conducted under the auspices of the RIPA. Covert surveillance is governed by a separate document, the Policy on the use of Covert Investigation Techniques.

3 Purpose

3.1 The purpose of this policy is to set out how MDDC manages, uses and operates SCS. MDDC uses SCS for one or more of the following purposes:

- To provide a deterrent to crime and anti-social behaviour
- To assist the prevention and detection of crime and apprehending criminals
- To improve public safety by reducing the perceived fear of crime
- To provide public reassurance and help improve quality of life in Tiverton
- To help secure safer areas and environments for those who live, visit, work, trade in or enjoy leisure pursuits in Tiverton
- To provide building security and a safe working environment for MDDC staff and visitors
- To provide MDDC vehicle fleet management information including the safety of staff and users of MDDC vehicles and assist in managing reported incidents and complaints
- To assist the police, other emergency services and MDDC with efficient management of resources

- To monitor traffic flow and assist in traffic management
- To assist with the MDDC's regulatory and statutory responsibilities, including revenues and benefits enforcement, civil parking enforcement
- To assist with the gathering and provision of evidence to support criminal and civil proceedings
- Support the management of public and commercial areas which are essential to commercial wellbeing of the community, including identifying bylaw contraventions
- To assist in civil emergencies and countering terrorism
- In appropriate circumstances, assisting the investigation of damage only accidents in MDDC owned car parks

3.2 The use of SCS must be a necessary and proportionate way of helping with a range of issues that affect people in public places, buildings and vehicles for which MDDC has a responsibility. MDDC also values the use of SCS to protect its staff where appropriate. MDDC must consider the nature of the problems to be addressed and that SCS are justified as an effective solution where it is used. MDDC will regularly evaluate whether it is necessary and proportionate to continue using SCS.

3.3 The Information Commissioner's Office ("the ICO") has enforcement powers which include the power to issue directives to remove or modify SCS installations. The ICO is supported by the Surveillance Camera Commissioner, which has issued a code of practice for the use of these cameras and which includes the guiding principles set out below.

3.4 This policy is approved by MDDC's Senior Management Team and Members.

4 Related MDDC Documents

a. Body Worn Video Procedure of Use
b. CCTV Code of Practice
c. Data Protection Policy
d. Freedom of Information Policy
e. Information Security Incident Policy
f. Code of Practice for management and operation of CCTV on Street Scene Vehicles
g. Code of Practice for operation and management of Body Worn Video Cameras
h. Records Management Policy
i. Removable Media Policy

5 Legal Framework

5.1 This policy provides guidance on the appropriate and effective use of SCS and in particular how it meets the requirements of:

a. The Human Rights Act 1998

b. Data Protection Act 2018

c. GDPR

d. RIPA

e. The Protection of Freedoms Act 2012 (PoFA)

f. Information Commissioners' CCTV Code of Practice

g. Surveillance Commissioner's Surveillance Camera Code of Practice

h. Criminal Procedure and Investigations Act 1996

i. Criminal and Disorder Act 1998

5.2 This policy applies to MDDC employees and any third party organisations shared services or individuals who are contracted to work on behalf of MDDC and in doing so have access to information or footage captured by SCS.

6 Surveillance Camera Code of Practice

6.1 MDDC will operate all SCS in line with the principles set out in the Surveillance Commissioner's Surveillance Camera Code of Practice:

a. Use of SCS must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

b. The use of SCS must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

c. There must be as much transparency in the use of SCS as possible, including a published contact point for access to information and complaints.

d. There must be clear responsibility and accountability for all SCS activities including images and information collected, held and used.

e. Clear rules, policies and procedures must be in place before SCS are used, and these must be communicated to all who need to comply with them.

f. No more images and information should be stored than that which is strictly required for the stated purpose of any SCS, and such images and information should be deleted once their purposes have been discharged.

g. 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.

h. SCS 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.

i. SCS images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

j. 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.

k. When the use of SCS 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.

l. Any information used to support SCS which compares against a reference database for matching purposes should be accurate and kept up to date.

7 CCTV and surveillance within the scope of this policy

7.1 MDDC acts as data controller for the SCS it operates for the purposes set out in section 3 above.

7.2 The cameras/systems within the scope of this policy include -

a) Tiverton Town Centre CCTV System (currently 40 cameras installed at various strategic locations throughout the town centre) *

b) Tiverton Multi-Storey Car Park, Phoenix Lane*

c) Phoenix House

d) Old Road Housing Depot

e) Carlu Waste Depot (Hitchcocks Business Park)

f) Exe Valley Leisure Centre

g) Lords Meadow Leisure Centre

h) Culm Valley Sports Centre

i) Body Worn Video

j) Street Scene Vehicles

7.3 Images from the cameras at (a) and (b)* above are sent to the CCTV CR in Tiverton, which accommodates the central switching recording and ancillary equipment for these systems along with the facility to monitor the system, if required. The images are transmitted over BT Fibre Optic cable to the Exeter City Council Public Spaces Surveillance CCTV Control Room at St Stephens House, Exeter where they are monitored both live and proactively and recorded in response to reported incidents or events. There is a formal agreement in place for Exeter City Council to undertake the monitoring of these cameras.

All material (data) controlled and managed at Exeter City Council remains the property of MDDC and is processed (data processing), under separate agreement, by competent, qualified Exeter City Council staff.

7.4 This policy does not apply to SCS where MDDC is not the data controller; for example, InPost lockers at the Leisure Centres and MDDC tenants' camera doorbells.

8 General Principles/Guidelines

8.1 MDDC's use of SCS accords with the requirements and the principles of the Human Rights Act 1998, the UK GDPR, the Data Protection Act 2018 and the PoFA. This policy recognises the need for formal authorisation of any covert 'directed' surveillance as required by the RIPA, and provides that SCS shall be operated fairly, within the law and only for the purposes for which it was established, or which are subsequently agreed in accordance with the Surveillance Commissioner's Surveillance Camera Code of Practice. The SCS shall be operated with due regard to the principle that everyone has the right to respect for his or her private and family life and home. Public interest in the operation of SCS will be recognised by ensuring the security and integrity of operational procedures which sit underneath it, and which balance the objectives of the SCS usage with the need to safeguard the individual's rights.

8.2 In accordance with the ECHR, the use of SCS must be necessary, in pursuit of a legitimate aim and in accordance with the law. It is therefore necessary to at all times consider the ECHR and a subject's human rights in the operation of this policy.

8.3 This policy ensures that the SCS used, managed or operated by or on behalf of MDDC meet the Surveillance Commissioner's Surveillance Camera Code of Practice by being:

8.4 Transparent

Wherever possible, the presence of SCS, the purpose for them and contact details for the controller of it should be clearly displayed to the public.

There are strict laws around the use of covert surveillance cameras, and these should only be implemented where necessary for a criminal enforcement purpose where MDDC has the necessary statutory authority and under the oversight of the SRO.

8.5 For a Legitimate and Specified Purpose

Prior to establishing any SCS installations, it is necessary to establish a legitimate purpose for it. The appropriate balance between the necessity of the SCS and the privacy rights of individuals can only be assessed in light of this intended purpose.

8.6 Proportionate to that purpose

The usage of SCS cameras, including field of vision and whether they can be remotely controlled, has to be proportionate to the identified need. For example, installation of a camera for the purpose of public safety would be unlikely to be proportionate in any area of no particular history of incidents.

SCS with audio/voice recording will not be installed unless found to be proportionate following a Data Protection Impact Assessment (DPIA). Where it is necessary to make voice recordings, signage will reflect that, save for in the case of BWV where in the interests of safety of MDDC officers and enforcement purposes, voice recording is usually present without such warning.

8.7 Privacy Risk Assessed

All existing and proposed SCS installations should be subject to a DPIA to identify what risks to privacy they pose and what controls can be applied to minimise these.

8.8 Subject to Senior Management Approval and Oversight

Proposals to install any new SCS will be discussed with the SPOC in the first instance. Thereafter, it shall be approved by a member of the senior management team, which may include the relevant manager for the service area. Where the DPIA indicates a high risk to privacy, then the approval of the SIO is required prior to the procurement of SCS equipment.

8.9 Secure from inappropriate access and interference

As SCS recordings contain personal (and sometimes special category) data, there is a legal obligation to ensure that access is limited to those with a genuine need and that any data held meets technical standards for information security. In the event of a data breach, then prompt steps will be taken, without undue delay, in accordance with MDDC's Information Security Incident Policy.

8.10 Subject to clear operational procedures which are binding on staff and contractors

All MDDC departments operating SCS are required to ensure that there are procedures in place which regulate where cameras can be installed, where they should point, under what circumstances data can be accessed or removed from the devices and under what circumstances it can be disclosed to other parties.

8.11 Auditable

All staff actions which effect the operation of SCS equipment should be captured in audit logs held on the devices or controlling applications. This includes any actions which change the field of vision, any downloads of footage and any deletion of footage. All SCS equipment must be specified so as to provide accurate time and date stamping.

All CCTV installations will be recorded on MDDC's CCTV Register.

8.12 Data Retention

SCS operated by MDDC shall normally retain footage for no longer than 31 days. Where footage is required for the purposes of prosecution of an offence or to defend legal claims, a copy should be made and stored securely. Footage will be saved to an encrypted external Hard Disc Drive/USB or equivalent or other secure remote storage medium in accordance with the Removable Disc strategy.

MDDC may be required by law to disclose SCS footage, without notification to the subject, in the interests of public security and in order to disclose information that is material to a legal case. All images that are relevant to a criminal investigation must be retained in accordance with the Criminal Procedure and Investigations Act 1996.

MDDC will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:

a. The SCS system being encrypted/password protected

b. Only authorised officers have access and are able to make copies of SCS footage in accordance with this policy and any relevant Code of Practice(s)

c. A log of any access to the SCS images, including time and dates of access, and a record of the individual accessing the images, will be maintained by relevant service RO. The log will be retained for six years.

8.13 Data Sharing requests

Where MDDC, as the data controller, has not delegated processing of SCS data to a data processor all requests for surveillance footage or images must complete the appropriate request form (available from the Information Management Team) and submit the form to the service area responsible for recording the footage and/or the Information Management Team and logged accordingly on the central log.

All data subject requests will be reviewed by MDDC's Information Management Team and determined according to a process which ensures compliance with legislation. For more details of how MDDC handles data subject requests, please see the Data Protection Policy, and information provided at Access to Information - MIDDEVON.GOV.UK.

9 Roles and Responsibilities

9.1 All officers with operational access to SCS equipment are responsible for following the specific operational procedures established for its use. This includes checking the equipment and reporting to the SPOC where it is found to deviate from the agreed specification or appears to have been interfered with.

9.2 Officers, contractors and other relevant persons shall only be permitted access to images obtained via SCS in accordance with this policy. Only officers with the appropriate authority shall have access to SCS systems. The viewing of live SCS images will be restricted to authorised officers in a controlled environment or such other live camera footage used by MDDC in public areas of their own buildings and as approved by the SIO or Monitoring Officer (or such person to whom delegates such approval to).

9.3 Recorded images which are stored by the SCS will be restricted to access by authorised members of staff with explicit powers to view images where viewed in accordance with the relevant Code of Practice. No other individual will have the right to view or access any SCS images unless in accordance with the terms of this policy as to disclosure of images.

9.4 All individuals with a need for operational access to SCS or for access to images captured via SCS shall be trained to a proficient level which meets appropriate safeguards before they are permitted access.

9.5 All relevant individuals are furthermore required to have read the Commissioner's Surveillance Camera Code of Practice and to have had sufficient training in the specific equipment they operate.

9.6 Officers are not permitted at any time to edit or alter SCS footage. The misuse of SCS could constitute a criminal offence.

9.7 Every individual with any responsibility for SCS under the terms of this policy or the relevant Code of Practice will be subject to MDDC's disciplinary procedures. Any breach of confidentiality may also be dealt with in accordance with those disciplinary rules.

9.8 The SRO is accountable for identifying a legitimate need for SCS installations where one exists (and for reviewing the same), for ensuring that DPIA are conducted and reviewed by the Corporate Management Team and an action plan generated and progressed and for making sure that risk controls are established where needed to protect personal privacy.

9.9 Members of the Corporate Management Team are responsible for approving proposed new SCS installations and any significant changes to existing ones. Where proposed installations are assessed as posing a high risk to personal privacy, they are responsible for referring the matter to the SIO for approval.

9.10 In cases of a serious breach involving SCS data, the SIO is responsible for reporting the matter to the ICO.

9.11 The SPOC is responsible for maintaining the SCS Register and participating in the investigation of breaches.

10 Review of this policy

10.1 This policy shall be reviewed every three years and as required to address legislative, regulatory, best practice or operational issues. However the Head of Finance, Property and Climate Resilience is given delegated authority to make minor amendments to the policy as required by legislative changes, formal guidance or local operational considerations.