Mid Devon District Council

CCTV Policy

Policy Number: HSG

October 2020

Version Control Sheet

Title: **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: **Group manager for Corporate Property and Commercial Assets**
abusby@middevon.gov.uk
Telephone number 01884 234948
Date: **October 2020**

Version Number: **1.0**

Status: **Draft**

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

Next review date: **October 2023**

Consultation **This document was sent out for consultation to the following:**
Group Managers
Cabinet Member
Property Services
Legal Services

``

Document History
This document obtained the following approvals.

Title	**Date**	**Version Approved**
Group Managers		
Leadership Team		
Community PDG	**November 2020**	
Cabinet	**January 2021**	
Council		
External consultant		

Definitions and Abbreviations

Systems Owner

Mid Devon District Council (MDDC) owns public space CCTV and a wide range of other smaller surveillance systems (PSS) operated across council business areas. The MDDC Group Manager for Property and Commercial Assets undertakes the responsibilities of ownership on behalf of MDDC.

Senior Responsible Officer (SRO)

The SRO is the Solicitor, Legal Services 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. The SRO will ensure that the interests of the council are upheld in accordance with this Code of Practice.

Data Protection Officer (DPO)

The MDDC Data Protection Officer ensures compliance with the EU General Data Protection Regulations (GDPR) and UK Data Protection Act 2018 (DPA18) and manages all rights of access to information on behalf of the Systems Owner.

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.

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.

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.

Surveillance Camera Code of Practice (SC Code) Code of practice local authorities must pay due regard to when operating surveillance camera systems, overtly, in public places.

CCTV Control Room (CR).

A secure facility located within Tiverton where connected CCTV and surveillance systems are managed and operated in the day to day management of public areas.

1. Introduction

1.1. The decision to install new or updated surveillance camera systems (SCS) will be supported by operational needs-assessment documentation and a Data Protection Impact Assessment to risk assess surveillance data processing and privacy issues. These documents will be completed before deciding to install.

1.2. All installations must be justified to meet a 'pressing need' where their use is being considered. Installation and use of SCS should be undertaken in consultation with the public, community organisations, council staff and the Police where appropriate.

1.3. 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 CCTV to protect its staff where appropriate. MDDC must consider the nature of the problems to be addressed and that CCTV is justified as an effective solution where it is used. MDDC will regularly evaluate whether it is necessary and proportionate to continue using CCTV.

1.4. All processes related to use of SCS will be regularly reviewed, at least annually, to ensure continued use of surveillance remains justified.

2. Scope

2.1. This policy applies to all MDDC owned public space CCTV and a wide range of other smaller surveillance systems (PSS) operated across Council business areas.

3. Related Documents

a. CCTV Code of Practice
b. Data Protection Policy
c. Freedom of Information Policy

4. Single point of Contact (SPOC)

4.1. MDDC has appointed a CCTV SPOC, the Facilities Manager for Corporate Property and Commercial Assets.

4.2. The SPOC will act as the main contact point for anything related to surveillance camera systems, and will ensure consistent, procedures and signage are applied to all sites at an operational level.

4.3. The SPOC will carry out an audit of the local authority schemes to find out exactly what type of systems are being used by the local authority across all schemes (e.g. CCTV, BWV, ANPR, UAVs and dash cams), where all its cameras are located and who has responsibility for them.

4.4. The SPOC will be responsible for maintaining a central register of all the public space surveillance cameras equipment that the local authority operates. The

register will include details of the location of each piece of equipment, its asset reference and the RO responsible for the equipment. This information will be collated from the individual asset lists provided through each site's CAP. The list should include cameras, monitors that display images and recording equipment. The SPOC will give each item of equipment an asset number so that it can be audited annually, and record if it is moved, removed etc. It is important to record whether or not the equipment is internal or external, and the purpose for each camera (e.g. crime reduction or public and staff safety)

4.5. The SPOC will maintain a register of the ROs appointed for each site. This is a record of the people authorised to access the system and the levels of access that have been approved. The SPOC is responsible for authorising individual's access levels and ensuring that regular reviews are undertaken to remove persons who no longer require the same or any level of access.

4.6. The SPOC will ensure that ROs are properly trained, keep them up to date on changes to legislation and help them to develop.

4.7. The SPOC must ensure all those who view images and/or operate cameras etc. have undertaken training on handling personal data and information security.

4.8. The SPOC must ensure that the Digital/Network Video Recorders (D/NVR's) used to record the images from all cameras are housed securely in the CR or in secure locations at the other MDDC sites.

4.9. The SPOC will carry out an annual desktop assessment of each site's Code Assessment Pack (CAP) to ensure it is complete and up to date.

4.10. The SPOC will complete an annual review to demonstrate that there is still a need to operate the scheme and all of the cameras connected to it, and that the scheme continues to be operated in compliance with relevant legislation and codes of practice. A questionnaire should be sent to each site's RO for completion on an annual basis.

4.11. Annual report – within the main CCTV annual report there should be a subheading for the SPOC to set out the number of sites under their remit and to give a brief overview of any inspections, contracts associated with the scheme, number of compliments and complaints in relation to the scheme and details of the scheme's performance and priorities, etc.

5. Responsible Officers (ROs)

5.1. A Responsible Officer (RO) must be appointed at each site or business area using surveillance systems. All ROs must sign a confidentiality agreement**.** The RO is responsible for the day-to-day management of the CCTV system and completing the annual questionnaire which is sent to them by the SPOC. The RO should identify through the questionnaire any changes to the system, whether the system remains fit for purpose and whether a maintenance contract is still in place for the system.

5.2. The RO is responsible for keeping the CAP for their site up to date which will demonstrate that their system continues to be operated in compliance with the CCTV Code of Practice, and present their evidence to the SPOC at the annual desktop assessment.

5.3. Typical CAP contents will include (but not limited to):

- Evidence of compliance with the principles of the SC Code and other relevant legislation such as RIPA, GDPR, DPA, and Human Rights considerations including completing the Self-Assessment Tool (provided by SPOC)
- Data Protection Impact Assessment (DPIA) - This should be reviewed whenever changes are made to the system (provided by SPOC)
- Document overview - This is a list of all the documents that the RO must maintain. They should record the date that they undertook the annual review of documents and any relevant comments
- An asset list - A list of the surveillance camera equipment that is used across the site. All surveillance cameras must meet the purposes agreed for their use and recordings must be of an appropriate quality so any issues should be communicated to the SPOC
- Declaration of compliance - Each RO must complete a declaration of compliance. They must confirm that the asset list is a complete list of all of the surveillance camera equipment on their site. This declaration must be completed annually (and on occasions where the RO changes)
- Records of access requests received – A log of who has asked to access CCTV images for the site
- Training records - The training the ROs have undertaken relevant to operating public space CCTV, and any standards required.
- Signage review – Annual review that all the signs which should be are in place and are not damaged. Signage should include details of the type of surveillance camera in use (e.g. CCTV, ANPR, etc.), the purpose of its use (e.g. to prevent and detect crime), that MDDC controls the scheme and contact details for further information.

6. Requests to access footage

6.1. The RO for each site must log all requests for access to information, this must include when the request was received, why and whether access was granted.

6.2. Access will be restricted; for example only allowing officers to view images on a monitor accompanied by the RO for the site, or an engineer might have access only under supervision.

6.3. Only ROs can download copies of recorded images when required for approved purposes, for example by the police or for a Freedom of Information (FOI) request. These images may then be kept (securely) for longer than the usual retention period in accordance with the relevant legislation.

6.4. Requests from the police should be referred to the CR and FOIs to Information Management who will both ensure that the correct disclosure request

documentation has been provided and completed properly before footage is released

6.5. If there are any issues with the footage this should be communicated to the SPOC as recordings must be of an appropriate quality to meet the requirements of the SC Code.

7. Disciplinary matters

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

8. Legal Framework

8.1. All our surveillance camera systems will be operated on a lawful basis and fully compliant with the requirements of the General Data Protection Regulations (GDPR) and the Data Protection Act (DPA) 2018; known as the 'data protection laws'. It will also fully regard all laws that impact on surveillance operations:

- The Human Rights Act (HRA) 1998
- The Crime and Disorder Act (CDA) 1998
- Freedom of Information Act (FOIA 2000
- Regulation of Investigatory Powers Act 2000
- Other Protection of Freedoms Act (PoFA) 2012
- relevant legislation according to specific use of CCTV in special circumstances (i.e. Covert use)

8.1. MDDC SCS including CCTV, body worn video (BWV), automatic number plate recognition (ANPR) and cameras fitted to council vehicles, will all comply with the Surveillance Camera Code of Practice issued by the Home Office (Section 29 PoFA) and other relevant legislation listed above.

Annex A – Technical Information

Mid Devon District Council CCTV Policy - Technical Requirement

Establishing the Purpose for a CCTV Requirement

1. There are five categories for classifying the purpose for CCTV cameras: -

    - **Monitoring:** to enable viewing of the number, direction and speed of movement of people/traffic across a wide area, providing their presence is known to the operator

    - **Detecting:** to enable the operator to reliably and easily determine whether or not any target (e.g. a person or vehicle) is present

    - **Observe:** to enable characteristic details of an individual, such as distinctive clothing to be seen, whilst allowing a view of activity surrounding an incident

    - **Recognising:** to enable the operator to determine with a high degree of certainty whether or not an individual shown is the same as someone they have seen before

    - **Identifying:** to enable identification of an individual beyond reasonable doubt

2. The image quality required for each of these purposes varies; further information on this and assistance in selecting equipment is available from the British Security Association (BSIA).

3. It should also be noted that if the equipment uses records sound/audio, this must not be used to record conversations between other people, although there are some limited circumstances in which audio recording might be justified, subject to sufficient safeguards.

4. 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's objectives.

5. CCTV schemes for Mid Devon District Council can be employed for 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 the District
    - To help secure safer areas and environments for those who live, visit, work, trade in or enjoy leisure pursuits in the District
    - To provide building security and a safe working environment for council staff and visitors

- To provide MDDC vehicle fleet management information including the safety of staff and users of council vehicles and assist in managing reported incidents and complaints
- To assist the police, other emergency services and MDDC with efficient management of resources
- To assist with the Council'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

6. Vehicle mounted CCTV is used to ensure the security and safety of the vehicle, employees, public and third party's property in the pursuance of delivering Council services and provide the driver with vision around the vehicle at all times. Surveillance Camera Systems mounted on vehicles may be used to enforce road traffic offences in the future.

7. Whilst body worn video (BWV) cameras and headcams are not strictly CCTV systems, the same restrictions with regard to the GDPR apply. Any Council service that is contemplating using BWV or headcams must consider whether there is a pressing need to capture images of people in this way. Videoing everyday life via such a system would be unjustified if there was no justification. The Information Commissioner expects any Council using BWV cameras to give people appropriate information that such a system is in use.

8. If covert cameras are to be used, this would need authorisation under the Regulation of Investigatory Powers Act (RIPA) 2000.

9. Once the purpose of the scheme has been identified it is necessary to: -

    - Ensure that everyone associated with the scheme is fully aware of its declared purpose, and the privacy implications of its use.
    - Ensure that the equipment is only used to achieve the declared purpose.
    - Decide whether constant real time recording is required or whether specific time periods may be more appropriate.

10. Cameras should only be used when necessary for the purpose(s) for which the system is being introduced. For example, if the cameras are used for enforcement purposes and to protect the safety of staff and the public, then officers would need to be provided with clear guidance on when to use the camera and how they should make the subjects of the surveillance aware that it is taking place.

11. If you are contemplating using such equipment, you must initially contact the MDDC SPOC propertyservices@middevon.gov.uk

Location of the Cameras

12. The location and siting of the Surveillance Camera System cameras is very important and must be designed carefully. The physical spaces 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 be installed in line with The Town and Country Planning Act 1990 - https://www.legislation.gov.uk/uksi/2015/596/schedule/2/part/2/crossheading/class-f-closed-circuit-television-cameras/made
    - Cameras must only monitor those spaces intended to be covered.
    - Cameras must be situated to ensure that they will effectively capture images relevant to the scheme's purpose.
    - If there is a risk of neighbouring spaces being monitored unintentionally the owner of such spaces must be consulted
    - Adjustable cameras which can pan/tilt/zoom, must be restricted to prevent operators from being able to allow unintended spaces to be overlooked and/or recorded.
    - Cameras must be able to produce images of sufficient size, resolution and images-per-second (ips) adequate for the purposes and suitable to provide evidence
    - Physical conditions and environment must be borne in mind when siting cameras, for instance taking into account lighting (or artificial enhancements with infrared/white light attached to the cameras) and the size of the area to be viewed and whether other obstructions such as trees will create blind hindrances.
    - The transmission medium for the camera system must be fit for purpose and able to transmit images at the suitable resolution without the reduction in image quality.
    - All necessary steps must be taken to protect the cameras from vandalism and theft.
    - Consideration will also be made to protecting the column or other support or street furniture to vandalism, bill posting and spray painting

13. It should also be noted that some areas have heightened expectations of privacy, such as changing rooms and toilets, cameras must only be used in most exceptional circumstances to address very serious concerns.

Signage

14. In order to comply with the GDPR, areas covered by CCTV schemes must display signs warning members of the public that a Surveillance Camera System is in use. Clear and prominent signs are particularly important if cameras themselves are discreetly located.

15. A good ratio of signs to cameras should be at least two for every PSS camera and one sign for every camera in premises/buildings/leisure/sports centres. Where possible, details of the location of the signs should also be recorded.

16. The wording and location of signage must take into account the following points: -

    - Signs must clearly identify to the public when they are entering an area covered by CCTV. These signs should be supplemented with further signs inside the area of required.
    - Signs must be clear, visible and legible both in terms of lettering and size, appropriate to the sign's location and who needs to see them (e.g car drivers or pedestrians)
    - Signs must identify: -
        - Who is responsible for the scheme
        - The scheme's purpose
        - Details of who to contact about the scheme

17. In exceptional circumstances it may be agreed that signage may compromise the purpose of the scheme especially where covert cameras are used. In such cases the owner of the scheme must consult with the Mid Devon District Council Data Protection Officer and Legal Services, and must identify and document: -

    - A specific criminal activity
    - The need for CCTV to obtain evidence of that criminal activity
    - The reasons why signage would prejudice success in obtaining such evidence
    - How long the monitoring should take place to ensure it is not carried out for longer than necessary

Equipment Quality/Technical Standards

18. Procedures and systems must be established to ensure that CCTV equipment is adequately maintained and that the quality of images recorded consistently meets the purpose of the scheme:

    - Recorded pictures and prints as well as live screens must produce good quality images and the quality must be regularly monitored.
    - If the system records information such as date, time and camera location, this data must be accurate at all times.
    - Equipment must be capable of being set up in such a way as to avoid inadvertent corruption.
    - Selection of equipment must ensure that copies of a recording can be made easily if asked for by a law enforcement agency and their use of the images should be straightforward.
    - A maintenance log must be retained for all equipment associated with the scheme.
    - If a camera is damaged or fails to operate correctly, there must be clear procedures for:

        - Defining who is responsible for ensuring repair/replacement.
        - Ensuring the camera is repaired/replaced within a specific time period.

- Ensuring the monitoring and documentation of maintenance work is provided.

Data Storage and Access

19. Retention periods must be established for required and non-required images and secure and controlled storage and access arrangements for images in compliance with the principles of Data Protection. These must be discussed with the Data Protection Officer, and must take into account the following points: -

    - Non-required images must be erased/overwritten within the prescribed time, being permanently deleted through secure methods
    - Required images must be retained for a length of time appropriate to their purpose and the purpose of the scheme
    - Systematic checks must be carried out to ensure compliance with the agreed retention period
    - When the documented period of retention has been reached images must be removed/erased
    - Any images that are to be retained as evidence must be kept in a secure location with controlled access
    - When images are removed for use in legal proceedings the following information must be logged: -

        - Date on which images/data were removed
        - The reason why they were removed
        - Any relevant crime incident number
        - The location of the images/data
        - Person taking custody of the images/data

    - Signature of the collecting police officer or other authorised person if appropriate
    - Monitors displaying images from areas where people would expect privacy must only be capable of being viewed by authorised employees of the User
    - Access to recorded images must be restricted to the designated member of staff responsible for the scheme who will decide whether to allow disclosure to third parties in accordance with the scheme's disclosures policy
    - Viewing of recorded images must take place in a restricted area with controlled access

20. When images are removed for viewing purposes the following information must be logged:-
    - Date and time of removal
    - Name of person removing the images
    - Name/s of the person/s viewing the images. If this includes third parties it must also include the third party's organisation
    - The reason for the viewing
    - The outcome, if any, of the viewing
    - The date and time images were returned to the system or to a secure area
    - All operators and others with access to images must be aware of the access procedures that are in place

Retention of Images Specific to the Use of Particular CCTV Systems

Recorded data relating to public space surveillance (PSS) systems should be kept no longer than 31 days before being overwritten unless this is saved to an external Hard Disc Drive (HDD)/USB or equivalent or other remote storage medium for evidential purposes. CCTV systems other than PSS should be kept for between 21 days before being overwritten, dependent upon the Operational Requirement (OR) and Data Protection Impact Assessment (DPIA).

The Council will adopt a consistent recording policy across all cameras used and recorded in their Council area; this should apply to cameras using both PSS within town centres and those in standalone corporate premises.