Thanet District Council

CCTV System Code of Practice

July 2019 - Version 7

July 2019 - Version 7 **1**
1.0 System Overview and Management 3
1.1 Introduction 3
1.2 Location 3
1.3 Signage 3
1.4 Purpose of CCTV 4
1.5 Aims 4
1.6 Management 5
1.7 Control Centre Personnel 5
2.0 The System 6
2.1 Introduction & Purpose 6
2.2 CCTV Coverage 6
2.3 Operational Details 6
2.4 Access to Network 6
2.5 Assessment of the System 7
2.6 Re-deployable or Mobile CCTV Cameras 7
3.0 Legislative Framework 7
3.1 Background 7
3.2 Human Rights Act 1998 7
3.3 General Data Protection Regulation 8
3.4 Regulation of Investigatory Powers Act 2000 (RIPA) 8
3.5 Right of Access 8
3.7 Access to and disclosure of images 9
4.0 Camera Siting, Image Quality and Data Access 11
4.1 Siting the Cameras 11
4.2 Processing of the images 11
5.0 Control Centre Use 12
5.1 Key Personnel 12
5.2 Control Room Access 12
5.3 Visitors' Book / Declaration of Confidentiality 13
5.4 Control Centre Physical Security 13
5.5 Communications 13
5.6 Council Complaints Procedure 13
6.0 Body Worn Video (BWV) 14
6.1 Introduction 14
6.2 Legislation 14
6.3 On Street Operational Guidance and Best Practice 15
6.4 Requests to View Footage 17

Authorised Version Control

Date	**Version**	**Comments**	**Authorised by**
8 July 2019	7.0	Body Worn CCTV Update	Head of Operational Services

1.0 System Overview and Management

1.1 Introduction

This Code of Practice aims to introduce measures to ensure accountability, high standards, good quality information and effective partnerships between the Police and the System owners/users. It is available to the public via the Thanet Council website.

The purpose of this document is to state the intention of the owners and the managers, on behalf of Thanet District Council CCTV Scheme as a whole and as far as is reasonably practicable, to support the objectives of the System and to outline how it is intended to do so.

All sections of the Code of Practice are subject to continuous review and reference should be made to the issue date shown on the front of the document. The Code of Practice is intended to reflect the spirit and guidance issued by the Information Commissioner's Office - In the picture: A data protection code of practice for surveillance cameras and personal information.

https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

The most up to date version of this guide is kept with this Code of Practice.

All recorded material is owned by Thanet District Council and will be subject to statutory conditions of the General Data Protection Regulations, Human Rights Act, Regulation of Investigatory Powers Act 2000 and in accordance with this Code of Practice.

The CCTV system will only be used to achieve the aims and objectives as set out in the Code of Practice. Cameras will at no time, without authority, be used to look into private residences/premises. No sound recording will be used in public places.

1.2 Location

This Code of Practice relates to the Closed Circuit Television System (CCTV) installed in the areas of Margate, Cliftonville, Ramsgate and Broadstairs, and operated by Thanet District Council.

The Control Centre is staffed by employees of the Council who will monitor and control the cameras 24 hours every day. The centre is located in Margate however the exact location is not disclosed to the general public.

1.3 Signage

In accordance with the General Data Protection Regulation, signage is in place informing the Public that they are entering a zone covered by surveillance equipment. Annual audit of signage will be undertaken.

1.4 Purpose of CCTV

The system provides coverage of retail, commercial, residential, recreational and open space areas located in the District of Thanet.

The purpose of the scheme is to help provide a safe public environment for the benefit of those people who live, work, trade, visit, service and enjoy the facilities of the town centres, foreshores, beaches and surrounding villages.

The system will be used for the provision of recordings for evidential purposes to the police and other bodies having prosecuting powers and, in some cases, insurance companies dealing with road traffic accidents.

This Code of Practice is supplemented by a separate Procedures Manual which is stored securely within the control room, and also accessible electronically, for use by Operators.

1.5 Aims

CCTV will play a major role in making the District safer helping to provide evidence where a crime has been committed and ultimately to reduce crime where cameras are operational. CCTV will help reduce the fear of crime.

The CCTV facility assists the Council in delivering the following Corporate Priorities;

1. Priority 1 - A clean and welcoming environment
   - Cleaner Streets and Open Spaces
2. Priority 2 - Supporting neighbourhoods
   - Safer Communities
   - Protecting and Improving Health For All
3. Priority 3 - Promoting inward investment and job creation
   - Strong and Diverse Economy

The region relies heavily upon tourism for its income. Residents and visitors to the region need to be reassured that it is a safe place to live and visit. CCTV is seen as a vital component in the Council's efforts to reduce the actual incidence of crime and to alleviate the perception of crime in the minds of the local and transient population.

The Objectives of the scheme are:-

• To assist in the detection and prevention of crime;
• To help provide evidential material for court proceedings;
• To deter those having criminal intent;
• To reduce the fear of crime and give confidence to the public that they are in a secure environment;
• To provide safer communities;
• To reduce acts of vandalism;
• To assist in the prevention and detection of antisocial behaviour that would deter members of the

public from using the regions facilities;
• To reduce vehicle related crime and anti-social behaviour in car parks;
• To assist with traffic management.

1.6 Management

The beneficial owner of the system is:- Thanet District Council (“The Council”) of : Cecil Street, Margate, Kent. CT9 1XZ

The Data Controller is:- Thanet District Council.

Control Centre General Enquiries:- Control Centre Supervisor (01843) 577000.

1.7 Control Centre Personnel

Thanet Council will be responsible for selecting and employing Personnel of high calibre to staff the control centre. They are selected using the criteria of standard job descriptions and person specification. In particular, employees are required to have qualities of personal integrity and each has to pass an enhanced Disclosure and Barring Service (DBS) check and necessary Police Vetting procedures.

All new employees undertake a minimum of two weeks of intensive in-house training on the operation and use of the system. Further training is given for operators to familiarise themselves with camera locations and local streets. In addition, each operator will attend a specialist training course run by an outside company in order to gain a CCTV operator’s licence, unless they already hold a current licence.

Only personnel who are fully trained or under supervised training in the use of the systems monitoring equipment, communication system and the operational and management procedures required under this Code of Practice will be permitted to undertake permanent duties on CCTV monitoring, and will hold or be in the process of obtaining a CCTV licence issued by the Security Industry Authority.

Employees work shifts covering 24 hours a day, 365/6 days per year. The minimum staff complement will always be sufficient to allow the control centre to function.

The control centre has electronic auditing procedures in place to randomly check that no misuse of the system is taking place and the necessary records are kept and that compliance with this Code of Practice is complied with.

All personnel working within the control room will complete an electronic duty log book showing the date and the start and finish times of their duty within the control room.

2.0 The System

2.1 Introduction & Purpose

The system provides CCTV surveillance in and around Margate, Ramsgate, Cliftonville and Broadstairs. Some images are transmitted via British Telecom's (BT) fibre optic network and some are IP cameras which transmit their images via radio to fixed fibre nodes for onward transmission to the control centre in Margate.

2.2 CCTV Coverage

The level of coverage in each of the areas with the Pan, Tilt and Zoom (PTZ) cameras is generally monitor and detection. With active patrols of vulnerable areas recognition or identification can be achieved. Coverage with the static cameras is monitoring and detection.

Total privacy within the surveillance area cannot be guaranteed however the cameras will not be used to unduly monitor persons going about their lawful business. Persons will only be specifically monitored if there is suspicion or knowledge that an offence has or may be about to occur.

2.3 Operational Details

The CCTV system operates 24 hours a day, 365/6 days a year and is constantly staffed by fully trained and dedicated Council personnel.

There is a direct radio link to the communications room at the Kent Police Headquarters. This allows access to Police Officers on the ground (through Control), and is sited on the main control desk in the CCTV control centre. The CCTV service will comply with the Airwave Service Code of Practice and holds the necessary TEA2 User Sub Licence (Unit no.5515005).

The CCTV control centre also has a direct radio link with the ThanetSafe Shop Watch and Pub Watch. This is a retailers' venture responding to the problems of shoplifting, pickpockets etc. There is positive Police input and Thanet CCTV system is an active member of this Shop Watch/Pub Watch scheme. We do assist in the apprehension and prosecution of shoplifters and other criminal offenders active in the Districts town centres.

2.4 Access to Network

The CCTV cameras located in Thanet are linked to the control centre via BT's fibre optic network or Broadband and can only be controlled, and recorded by authorised personnel in that control centre. A limited number of camera feeds are available to Margate Police Station for operational purposes.

2.5 Assessment of the System

The “Owner” is responsible for ensuring that the system is evaluated periodically, a minimum of a once per annum basis.

Evaluation will include statistical reports on the number of:-

• incidents monitored

• incidents reviewed

• evidence provided

• camera location reviews

2.6 Re-deployable or Mobile CCTV Cameras

From time to time re-deployable or mobile cameras may be temporarily sited within the Thanet District. The use of such cameras, and the data produced by virtue of their use, will always accord with the objectives of the CCTV System and be governed by this Code of Practice and the operational procedures for Thanet District Council CCTV Centre.

3.0 Legislative Framework

3.1 Background

The system is registered with the Information Commissioner under the General Data Protection Regulation. The latest certificate is available on the website of the Information Commissioner. Thanet District Council recognises that the use of CCTV could potentially impact on a member of the public’s right to respect for private and family life afforded by Article 8 of the European convention on Human Rights and the Human Rights Act 1998. CCTV will therefore only be used for the prevention and detection of crime or disorder, to ensure public safety or to maintain safety within and around the district. CCTV for covert or targeted surveillance purposes will be carried out in accordance with the Regulations of Investigatory Powers Act 2000 (RIPA) and will be subject to the appropriate authority levels.

3.2 Human Rights Act 1998

This code will observe Articles 6 and 8 of the Human Rights Act 1998 and will incorporate those safeguards necessary to protect the rights of privacy, except where the law permits specific surveillance activities.

3.3 General Data Protection Regulation

All Closed Circuit Television (CCTV) schemes that receive, hold or process data about a known person are obliged to conform to the General Data Protection Regulation. The Act covers CCTV systems used in areas where the public would have a “right to visit” and requires that personal data must be:-

(a) “Processed lawfully and fairly and in a transparent manner in relation to an Individual;

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

(d) Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regards to the purposes for which they are processed, are erased or rectified without delay;

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the
appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

Article 5(2) requires that “The controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

3.4 Regulation of Investigatory Powers Act 2000 (RIPA)

When it is necessary to carry out 'DIRECTED OR COVERT SURVEILLANCE' the appropriate authority will be obtained from the relevant authority.

3.5 Right of Access

(Subject Access Request)

Under GDPR individuals will have the right to obtain:-

• Confirmation that their data is being processed;
• Access to their personal data; and
• Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see article 15 of the GDPR)

Who receives the initial enquiry

Subject Access Requests should be sent to the Data Protection Officer and information is available on the Council's website.

https://www.thanet.gov.uk/info-pages/subject-access-requests/

Charges

A copy must be provided free of charge however a "reasonable fee" may be charged if the request is manifestly unfounded or excessive or particularly if it is repetitive.

Response times

The information must be provided without delay and at the latest within one month of receipt.

3.6 Freedom of Information Requests

• Freedom of information requests should be addressed to the Data Protection Officer and details of this is available on the council's website;
https://www.thanet.gov.uk/info-pages/freedom-of-information-request/

• The information must be provided without delay and at the latest within 20 working days of receipt.
• A copy of the response must be sent to the FOI officer.

3.7 Access to and disclosure of images

General Policy

All requests for the release of data shall be processed. All such requests shall be channelled through the Operational Services Enforcement Manager, although day to day responsibility may be devolved to the Control Centre Supervisor.

Request to View Data

a) Primary requests to view data generated by a CCTV System are likely to be made by third parties for any one or more of the following purposes:

Providing evidence in criminal investigations or proceedings (Police and Criminal Evidence Act 1984 (9), Criminal Procedure and Investigation Act 1996 (7).

- Providing evidence in civil proceedings.
- The prevention of crime and disorder
- The investigation and detection of crime (may include identification of offenders)
- Identification of witnesses
- Public Interest

b) Third parties, which are required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:

- Law Enforcement Agencies
- Statutory authorities with powers to prosecute, (e.g. Customs and Excise; Streetscene; Trading Standards, etc.)
- Solicitors
- Plaintiffs in civil proceedings
- Accused persons or defendants in criminal proceedings
- Insurance companies in connection with road traffic incidents
- Other agencies, as specified in the Code of Practice according to purpose and legal status.

c) Media disclosure - There is generally no release of data to the media in the event of a request from the media for access to recorded material. Data may be released to the media, to educate the public on certain offences, to promote public safety, to protect staff and contractors, where it is decided that it is in the public's interest or that the public's assistance is required to identify a victim or perpetrator in relation to a criminal or anti-social behavioural incident.

d) Viewing of Images - As the scheme is registered with the Information Commissioner it is necessary to provide a viewing station away from the Control room, or in an area to protect the images of other individuals on the recordings being disclosed. Viewing room is identified as the meeting room found in the secure access Enforcement Hub in Margate, or alternatively the secure PACE interview room on 2nd floor of Council Office in Margate.

e) Disclosure of images - Where images are disclosed to a third party, they become the data controller for their copy/ ie of the image/s and are responsible for compliance with GDPR.

4.0 Camera Siting, Image Quality and Data Access

4.1 Siting the Cameras

Cameras have been sited to provide surveillance of the town centres, foreshores, main beaches, selected car parks, civic offices, and in some cases, the surrounding areas of Thanet. The system comprises of a mixture of Pan Tilt Zoom (PTZ) and Static functionality.

Static camera installations provide a fixed field of view of a particular scene e.g. an area of a car park or stairwell. Fully functional installations provide (PTZ) functionality and can be utilised to monitor a range of scenes under operator / automatic tour or preset control.

A number of PTZ installations are situated within residential areas. However these cameras will be controlled in accordance with the Operational Procedures Manual and all operators will be fully aware that they are only able to use the equipment in order to achieve the purpose(s) for which it has been
installed. In certain circumstances or upon approved request, it is a function of the equipment that parts of specific scenes may be electronically “blanked” from providing a view of an area.

4.2 Processing of the images

All new installations and upgrade of existing cameras will be commissioned in line with a privacy impact statement to ensure that the cameras deliver the correct field of view and are of adequate quality for their particular requirement.
High quality equipment has been installed in 2017/8 throughout the Districts system.

Images will not be retained for longer than is necessary. They are stored in digital format on hard drives for a period of 31 days. After this time the images are erased.

Only authorised personnel in the control centre can access the data stored on the hard drives.

All data will be handled in accordance with this Code Of Practice (COP) and reference should be made to the Operational Procedures Manual. All operators of the system will be fully trained in handling and processing data.

Evidential images will be provided on DVDs or USB flash drives which are referenced and recorded on Request For CCTV Recorded Material Form, located in control room. This is to prevent the unlawful release of footage.

Photographs (or still images) will be processed in the same way as footage and be only taken for a specific reason from an authorised partner. The DVD, USB flash drive and photograph will remain the property of Thanet District Council until collected and signed for. Any DVD or photograph will be destroyed after 3 calendar months from original request if not collected from the control room by the requesting officer. CCTV Supervisor is responsible for ensuring compliance with this directive.

5.0 Control Centre Use

5.1 Key Personnel

System Manager

The control centre is managed locally by a manager with direct control of the scheme. The system manager retains responsibility for the implementation of procedures to ensure that the system operates according to the purpose for which it was installed and in accordance with the objectives identified for the system.

Control Room Supervisor

The supervisor has a responsibility to ensure that at all times the system is operated in accordance with the policy and all procedural instructions relating to the system, and for bringing to the immediate attention of the manager any matter affecting the operation of the system, including any breach or suspected breach of the policy, procedural instructions, security of data or confidentiality.

5.2 Control Room Access

Only visitors with a valid reason will be allowed access to the control room and monitored areas. Public access to the monitoring and/or recording facility will be prohibited except for lawful, proper and sufficient reasons and only then with the personal authority of the System Manager or Supervisor. Any such visits will be fully supervised by the Manager or Control Room Supervisor.

Police Access

Police Officers will be granted 24 hours access to the control room and monitoring area for the purpose of retrieving evidence, advising on criminal intelligence, operational, liaison and security purposes in line with the Service Level Agreement between Thanet District Council and Kent Police.

Contractor Access

Only trained and authorised personnel will be granted access to the control room or monitoring areas for the purpose of system maintenance.

Inspectors/Auditors Access

The Control Room Supervisor will carry out a monthly audit of the CCTV centre ensuring that procedures are followed. The Council's auditors carry out an audit on the CCTV Service every 3 years. These visits may take place at any time without prior warning.

5.3 Visitors' Book / Declaration of Confidentiality

ALL non-authorised visitors will be required to sign a visitors' book located in the CCTV Control Room. Visitors are required to make an undertaking that all information witnessed during their visit will be held as confidential.

5.4 Control Centre Physical Security

Authorised personnel will normally be present at all times when the equipment is in use. If the monitoring facility is to be left unattended for any reason (i.e. bomb threats/fire drills/staffing etc) the room must be secured and grab bag taken by operator.

5.5 Communications

A number of separate communication systems will be in operation within the control centre. All systems are to be used strictly in accordance with operating procedures laid down by the suppliers/users. For Police radio systems UHF/VHF and AIRWAVE the procedures and protocols will be supplied by the relevant Police Department (i.e. Communications) and the Council has been added to the Police Airwave Sharers List and holds a TEA2 licence. Any misuse of Police Systems within local authority/partnered control centres may lead to the removal of that system and/or disciplinary measures.

The shop/pub watch radio licence is covered on the registration of the shop and pub watch OFCOM registrations.

In the event of an incident being observed by a CCTV operator, contact will be made as per the procedures laid down either by radio/telephone.

5.6 Council Complaints Procedure

CCTV is no different to any other department within Thanet District Council. We want to provide the best possible services for all residents and visitors to the District. Therefore we need to know if there is a problem or if there are specific concerns about our service delivery. Equally we would like to hear
from people who are pleased with the service.

Our comments and complaints system operates on three levels:
• Stage 1: Looked into by the relevant service manager and you will receive a response from the Executive Support Unit
• Stage 2: Looked into by a Head of Service or Director and the response will be sent to you from the Executive Support Unit.
• Stage 3: Looked into by Local Government and Social Care Ombudsman.

There are two separate forms and can be obtained by visiting the Council's website

https://www.thanet.gov.uk/services/complaints-compliments/

6.0 Body Worn Video (BWV)

6.1 Introduction

This section sets out the Council's Policy and Procedural Guidelines for the use of Body worn CCTV cameras by Civil Enforcement Officers (Parking). It enables employees to comply with the relevant legislation relating to video recording and outline the associated benefits to Civil Enforcement Officers (Parking) and the general public. It also documents best practice procedures with regard to integrity of data, images and video as well as its security and use.

The use of Body worn CCTV can provide a number of benefits which include a deterrent to acts of aggression or verbal and physical abuse toward Civil Enforcement Officers (CEOs), and providing evidence to support Police investigations. Body worn CCTV forms part of a CEOs Personal Protective Equipment and is provided solely for Health and Safety purposes. It will be used in an overt manner and emphasised by CEOs wearing clear identification that it is a CCTV device. Prior to commencement of any recording, where possible, CEOs will give a clear verbal instruction that recording is taking place.

Body worn CCTV will not be used to gather evidence for Parking Enforcement purposes nor will it be used as evidence in proceedings against any member of staff.

6.2 Legislation

The integrity of any video data recorded will be considered in accordance with the following legislation:

Data Protection Act 1998
Freedom of Information Act 2000
Human Rights Act 1998
CCTV Code of practice 2014

Data Protection Act 1998
The Information Commissioner's Office is the regulator for the Act and has given guidance with regard to CEO use of Body worn CCTV equipment. This legislation regulates the processing of 'personal data' or 'sensitive personal data' whether processed on computer, CCTV, still camera or any other media. Any recorded image that is aimed at or may identify a particular person is described as 'personal data' and covered by this Act and will include images and audio captured using Body worn equipment. The use of Body worn CCTV in this guidance is 'overt use' meaning that equipment is not to be worn or used in a hidden or covert manner.
Where an individual asks to view footage this is called a 'Subject Access Request' (see 6.4)

Human Rights Act 1998

Article 6 provides for the right to a fair trial. All images captured through the use of a Body worn device have the potential to be used in court proceedings and must be safeguarded by an audit trail in the same way as any other evidence. Article 8 of the Human Rights Act 1998 concerns the right for private and family life, home and correspondence. Recordings of persons in a public place are only public for those present at the time and can still be regarded as potentially private. Any recorded conversation between members of the public should always be considered private and users of Body worn equipment should not record beyond what is necessary when recording a confrontational situation.

The Council ensures that the use of Body worn CCTV is emphasised by CEOs wearing it in a prominent position (normally on their chest) and that its forward facing display is visible to anyone being recorded. Additionally, CEOs will wear identification that it is a CCTV device and make a verbal announcement, where practicable, prior to commencement of any recording. The Council will adhere to the CCTV code of practice 2014 in all aspects referring to Body Worn Cameras.

6.3 On Street Operational Guidance and Best Practice

Training

All CEOs will receive full training in the use of Body worn CCTV. This training will include practical use of equipment, on street operational guidance and best practice, when to commence and cease recording and the legal implications of using such equipment.

Daily Use

Body worn CCTV will only be used in the event where CEO`s find themselves in a confrontational situation where they are subject to, or feel that they are likely to be subject to, verbal or physical abuse. Recordings will not commence until the CEO has issued a verbal warning, where possible, of their intention to turn on the Body worn device.
Recordings will not be made whilst performing normal patrolling duties.
All recordings will be held securely.
Access to recordings will be restricted to authorised personnel in the Parking Team and Senior Managers responsible for Parking Services.

Start of Shift Procedure

All CEOs will be issued with their own Body worn CCTV device. At the commencement of each shift it will be the CEOs responsibility to verify that the unit is fully charged and that the date and time displayed is correct. Any discrepancy in the Date or Time should be bought to the attention of the Civil Enforcement administrative staff.

Recording

Recording must be incident specific. CEOs must not indiscriminately record entire duties or patrols and must only use recording to capture video & audio of specific incidents. For the purposes of this guidance an ‘incident’ is defined as:

a) An engagement with a member of the public which in the opinion of the CEO is confrontational, and where the CEO believes they may be subject to physical or verbal abuse.
b) The CEO is approached by a member of the public in a manner perceived as aggressive or threatening. At the commencement of any recording the CEO should, where possible, make a verbal announcement to indicate why recording has been activated.

The purpose of issuing a verbal warning is to allow a member of the public to modify any unacceptable confrontational or aggressive and threatening behavior. If, at any time during an incident the CEO considers that the use of Body worn CCTV or the issuing of a verbal warning, is likely to inflame a confrontational situation, the CEO may use discretion to disengage from further discussion and withdraw from the incident.

A specific form of words to be used in any warning to a member of the public has not been prescribed, but CEOs should use straightforward speech that can be easily understood by those present such as ‘I am wearing a Body worn CCTV camera and I am now recording’.

Playback

CEOs will need to be fully aware of the legal implications once digital images and audio have been recorded. To this end playback should only be at the request of a Police Officer attending the incident or by another police officer subsequently involved in the investigation of the incident. Any request to view captured video by a member of the public, will need to be made in line with the ‘subject access
procedure’.

End of Shift

CEOs should ensure that any CCTV footage required for evidential purposes has been correctly bookmarked and that any necessary The Action Manager (TAM) Incident Reports have been completed. They will also be responsible for ensuring all Body worn devices have been connected correctly to the docking station to enable downloading and charging.

Storage of Data

All recorded footage will be uploaded to the Body worn camera software system (DEMS) on the dedicated and secure laptop located in the Civil Enforcement office by the Parking Policy Officer. They also will ensure that any footage to be retained has been correctly bookmarked and that supporting TAM Incident Reports have been completed.

For Incidents where the Police have not been in attendance the Uniformed Services Manager or Authorised personnel (as below) will review the recording and in consultation with the CEO operating the device a decision will be made on whether referral to the Police is appropriate.

The Parking Policy Officer will then transfer the data from DEMS on to a DVD-R and complete the CCTV Recorded Information Form. All retained data will be kept until all investigations have been completed or a prosecution has taken place. Any other data not required for evidential purposes will be deleted by the Parking Policy Officer as soon as practicable.

Authorised Personnel
Head of Service Operational Services
Operational Services Enforcement Manager
Parking Policy Officer
CCTV Supervisor

6.4 Requests to View Footage

Subject Access Request

All data not required for evidential purposes will be deleted upon download. However, the Data Protection Act gives individuals the right to be told what personal information we hold about them and to receive a copy of that information.

Any application to view footage is covered by Thanet District Councils 'Subject Access Request' procedure.

Details can be found here - https://www.thanet.gov.uk/info-pages/subject-access-requests/