OPERATING PROCEDURES MANUAL CCTV 2021

Tendring
District Council

VERSION CONTROL SHEET

Title	CCTV Operating Procedures
Author	Claire Ellington
Approved by	CCTV SRO & Internal Audit Manager
Date	02/02/2021
Version Number	3
Status	Draft
Review Frequency	Yearly
Next Review Date	21/04/2021

AMENDED HISTORY / CHANGE RECORD

Date	Version	Key Changes/Sections Amended	Amended by
17/09/2019	1		CE
21/04/2020	2	Amended to reflect responsibilities in other TDC departments	CE & MW
02/02/2021	3	Yearly review	MW

CONTENTS

CCTV OPERATING PROCEDURES MANUAL

MISSION STATEMENT

To provide a safe and secure environment in those parts of the district, and Council owned buildings, covered by CCTV Systems, for the benefit of all those living in, working in, and visiting the area.

FOR THE PURPOSE OF THIS MANUAL, AUTHORISED RESPONSIBLE STAFF ARE:

OTHER AUTHORISED STAFF WITH LOCAL RESPONSIBILITY:

CCTV Control Centre

- Control Centre Supervisor
- Senior Control Centre Operator

Leisure Centres - Clacton, Walton, Dovercourt, Bightlingsea

- Assistant Director Economic Growth and Leisure
- Sports Facilities & Business Manager
- Duty Officer

Civic Buildings, Depots and other Council owned premises

- Corporate Director, Operations and Delivery
- Facilities Manager
- Technical Officer - Facilities Management

The cameras in the Leisure Centres, Civic Buildings and other Council owned premises can only be viewed locally on site (known as stand-alone systems); the Control Centre does not have access to view video feeds from these. The General Principles below apply across all TDC owned CCTV systems, however there are specific procedures that apply to the stand-alone systems.

GENERAL PRINCIPLES

This section covers the general principles for the operation of CCTV systems used for the surveillance of public areas.

All users are to be fully conversant with the Tendring District Council (TDC) CCTV Code of Practice and the CCTV Operating Procedures Manual, before operating the system. All CCTV Operators and Authorised Persons should sign to confirm that they have read and understood these documents, and that they agree to abide by their instructions. Upon signing, each Operator or Authorised Person will assume responsibility for their own actions with regards CCTV. Due to the legal requirements now in place, variation from the codes may make the CCTV Operator and Authorised Person liable to legal redress and disciplinary procedures.

CIVIL LIBERTIES-HUMAN RIGHTS- DATA PROTECTION GDPR (GENERAL DATA PROTECTION REGULATION)

CCTV Operators are to be particularly careful when dealing with issues concerning Civil Liberty and Human Rights. Legislation is in place to protect individuals' rights. Tendring District Council clearly wishes to protect these rights.

The EU General Data Protection Regulation (GDPR) supplemented by The Data Protection Act 2018, and accompanying Information Commissioner's code of practice for CCTV, regulate the management and operation of public area CCTV systems. The CCTV Code of Practice deals with the conditions it places upon CCTV schemes more fully. If there is any doubt as to the action taken by CCTV Operators, reference must be made to a member of Responsible Staff.

In compliance with Protection of Freedoms Act 2012 the Surveillance Camera Commissioner issued a code of practice for CCTV, which has been incorporated into the Tendring District Council's CCTV code of practice and this operating procedure manual.

This code sets out 12 guiding principles that provide a framework for operators and users of surveillance camera systems, so that there is proportionality and transparency in their use of surveillance and the systems are capable of providing good quality images and other information that are fit for purpose.

The increase in the capability of surveillance camera technology has the potential to increase the likelihood of intrusion into a person's privacy. The Human Rights Act 1998 gives effect to the rights set out in the European Convention on Human Rights. Some of these rights are absolute, whilst others are qualified, where it is permissible for the state to interfere so long as it is in pursuit of a legitimate aim and proportionate. Article 8 (Human Rights Act 1998) establishes the qualified right to privacy, where a person's rights may be restricted for specified reasons, such as to protect public safety or to prevent disorder or crime; at the same time, a public authority like the Council must take positive steps to protect a person's privacy.

SECURITY OF IMAGES AND DOCUMENT COPYING GENERALLY

- CCTV Operators should also be particularly careful when dealing with all recorded material.
- Under no circumstances should Operators allow the original recording of images to be taken from the recording site (to seize hard disks from the digital recording system) without specific authority. No Police Officer of whatever rank is authorised to remove digital images without authority and only in accordance with the Codes of Practice.
- CCTV Operators will ensure that no additional copies are made other than in accordance with the Code of Practice and Data Protection Act 1998.
- Where copies are made, the person receiving must sign for them and be made aware of the implications of complying with the Data Protection Act guidelines.
- Document copying also falls within the Data Protection Act and due regard must be given to those guidelines. A copy of the recorded images is a document as defined by Police and Criminal Evidence Act (PACE)

If in doubt, CCTV Operators should ask a member of Responsible or Authorised Staff.

AIMS & PURPOSE OF THE CCTV SYSTEM

This section deals with the overall objectives of the provision of the CCTV system in the Tendring District.

BASIC PURPOSE OF THE CCTV SYSTEM

The purpose of this CCTV System is to assist in the prevention, detection and prosecution of crime and public order.

AIMS OF TENDRING CCTV SYSTEMS

The aim of the CCTV Systems is to monitor public areas in Tendring to provide assistance with the following:-

- The prevention and detection of crime;
- To reduce incidence of nuisance, anti-social behaviour, vandalism and graffiti;
- To gather intelligence and identify suspects;
- The maintenance of public order;
- To reduce the fear of crime;
- To improve Police Officer, the public and employees health and safety;
- To promote safer communities;
- To assist in the training of Local Authority staff in respect of CCTV Operation;
- Undertake locally agreed assignments provided they adhere to current legislation and the Code of Practice;
- To provide appropriate information for Town Centre management;

BASIC FUNCTIONS OF THE CCTV SYSTEM

These functions will be aided through the provision of the CCTV System being:-

- A deterrent to criminal and anti-social behaviour;
- Able to provide 24 hours surveillance;
- A visual guide allowing an assessment of the Police response to incidents;
- A means to gather evidence for court;
- Able to assist with training of CCTV Operators and Police Officers;
- Any other function agreed by the Senior Responsible Officer in consultation with the Community Safety Partnership and the Portfolio Holder for Housing.

SYSTEM EVALUATION

Evaluation of the benefits of the system will take place on an annual basis. Statistical information regarding the use of cameras and evidence gained from Police insight will be used during this evaluation. Overall responsibility for the operating of the CCTV System is the responsibility of Tendring District Council.

PUBLIC CONFIDENCE IN THE SYSTEM

Legitimate public concerns exist over the use of CCTV and many of the specific guidelines below are designed to satisfy the community that the use of cameras are subject to adequate supervision and scrutiny. It is of fundamental importance that public confidence is maintained by fully respecting individual privacy.

OVERALL LIABILITY

Whilst every effort will be made to monitor the System by the CCTV Operator, Tendring District Council will not accept liability for any occurrence which is not observed by an Operator.
(Note: This does not create implied liability for any observed incidents. Consequent actions taken by Essex Police to reported incidents should comply with their current policies, over which Tendring District Council has no control).

ACCESS TO THE CCTV CONTROL CENTRE

CONTROL OF ACCESS TO CONTROL CENTRE - GENERAL

The Control Centre includes operator workstations, a monitor wall and review suite. Access will be limited to those personnel authorised to attend the Control Centre. All persons attending, except those people with authorised access, must complete the Visitors Log.

CONTROL OF VISITORS

Visitors from outside organisations must be accompanied by a member of Authorised Staff or designated member of staff who will be responsible for them at all times. It will not be the responsibility of the CCTV Operators to supervise such visits. All visitors will be required to sign the Visitors Log and undertake to abide by the implications of the Data Protection and Human Rights Acts. Visitors may be asked to leave if an incident is being monitored in order to comply with the Data Protection Act.

CONTROL CENTRE STRUCTURE AND SUPERVISION - GENERAL

DEFINITION OF SUPERVISORY STRUCTURE AND DISCIPLINES

Tendring District Council is responsible for the management and operation of the CCTV Control Centre. The CCTV operators and Control Centre managers are employed by Tendring District Council.

CCTV Operators should communicate with a member of the Authorised Staff if they have any questions or problems.

Members of the Authorised Staff are responsible for CCTV Operator development and staff appraisals etc.

INCIDENT DE-BRIEFING FOR CCTV OPERATORS

Due to the systems capability to produce high quality pictures in real time, occasions may arise where the CCTV Operators witness graphic and traumatic events. It is the responsibility of the Authorised Staff to ensure that CCTV Operators, in such circumstances, attend critical debriefings and are made aware of the assistance that is available to them via Human Resources. This is mostly delivered through the Employee Assistance Program (EAP) and is available to all staff..

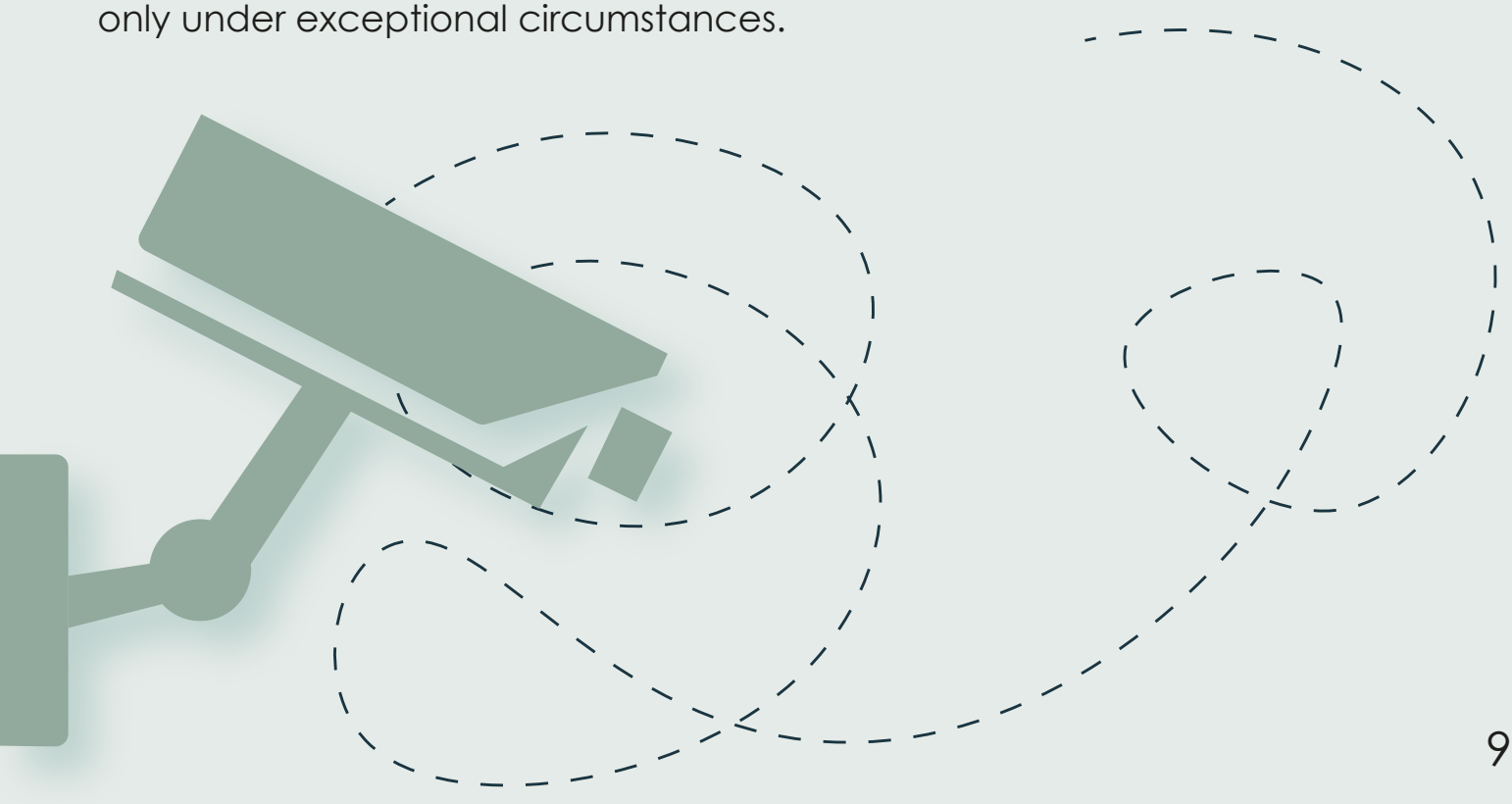
CCTV OPERATORS RESPONSIBILITIES AND DUTIES – GENERAL

OVERALL RESPONSIBILITY

The list given below indicates the responsibilities and duties of the CCTV Operators. This will include the definition of appropriate reactions to the camera equipment monitors. It is assumed for the purpose of this checklist that the CCTV Operator has at least attended and passed a local basic training course of CCTV operation. It is also essential to ensure that the Operator has access to this Operating Procedures manual and Codes of Practice for the Control Centre.

CONTROL CENTRE CONDITIONS

a) The consumption of food or drink is only permitted in the break-out area of the Control Centre, away from electronic equipment.
b) Smoking is not permitted within the Control Centre
c) CCTV Operators are not permitted access to the equipment room unless specifically authorised to do so by a member of Authorised Staff and even then only under exceptional circumstances.



RESPONSIBILITY OF THE CCTV OPERATOR

The CCTV operator:

a) Must have the appropriate working knowledge and skill to operate equipment within the Control Centre for which they are responsible and ensure that such equipment is in working order at the commencement of each shift. Fault records and procedures exist on the J: drive and in the CCTV Manual.

b) Should have an outline knowledge of other equipment in the Control Centre not associated directly with their duties.

c) Should have a clear understanding of the system, the number and location of cameras, the areas of the Town Centre, Seafront, Car Parks, and Council owned buildings covered by the cameras and whether a particular camera is fully functional or not. They should also have an understanding of other systems, including car park management and emergency phone lines operated by the Control Centre.

d) Have a clear understanding of the operational requirements for each camera (the purpose and scope of each camera).

e) Must ensure that all Control Centre logs are completed in a timely manner. Incidents are to be fully described and logged as indicated below. These may be required as evidence in court and as such should not contain matters of opinion.

f) Must be aware of civil and criminal law as it relates to the type of incidents likely to be observed by the CCTV System. In cases of doubt, the advice of a member of Authorised Staff should be sought.

g) In the interest of Health & Safety, CCTV operators will not interfere with any equipment for which they have not received training.

h) Any accidents that occur within the Control Centre will be reported to a member of Authorised Staff without delay and recorded in the Control Centre accident book. Normal Health & Safety rules will apply in the Control Centre.

RECORD KEEPING ASSOCIATED WITH CONTROL CENTRE ACTIVITIES

The following logs are to be maintained by the Control Centre staff.

Visitor's log,

Incident log

Maintenance fault log – J: Drive & Folder

CCTV Creation log & witness statement

CCTV footage request (pro forma)

Non-executed log (pro forma)

INCIDENT LOG

CCTV Operators will be responsible for keeping a record of all incidents and events whilst operating the system. Once completed it is retained for evidential purposes.

The Incident log contains matters of evidential value and as such must be maintained in a true and accurate manner. It must not contain offensive or spurious comments. Extracts may be served on the defence and must include fact only and **not matters of opinion.** The log will run chronologically and must not have delayed entries made without comment. It is important that in all cases, the description recorded in a log of a suspect is that of the "first given". Any inaccuracies may prejudice the court case later. (Criminal Procedures and Investigation Act (CPIA)).

In the event that a discrepancy is found on any of the system clocks the CCTV Operator will notify a member of Authorised Staff for advice. Discrepancies and action taken will be entered in the Incident Log or, if it is established that a fault has occurred, in the Maintenance Fault Log.

VIEWING

CCTV Operators will ensure that all persons using the review facility complete either the CCTV Creation Log or the Non-executed Log. Completed logs will be retained in secure storage. Only those staff with a valid reason to view data will do so (Data Protection Act 7th Principle).

COPYING

Any authorised person requiring a hard copy of an image or photograph must complete a CCTV Proforma. Under no circumstances will copies be made or photographs produced without this form being completed satisfactorily. The authorised person should state clearly the reason for such a request, the appropriate information for the Operator to locate the relevant portion of the media or stored image and any other information to assist the CCTV Operator to produce copies. Without such information, the request may be refused. Only essential requests will be processed.

MAINTENANCE AND FAULT LOG

When a fault is identified on the system, it is to be reported to the maintenance contractor immediately. The maintenance contractor is required to complete the repair within specified times following the report and it is important that the performance targets are not lengthened unnecessarily.

Following completion of a repair, the Contractor's engineer will demonstrate the satisfactory completion of the repair and mark the job as completed on the CCTV Fault log.

In all cases a notice must be displayed in the monitoring area that engineers are at work on the system. This is a Health & Safety requirement.

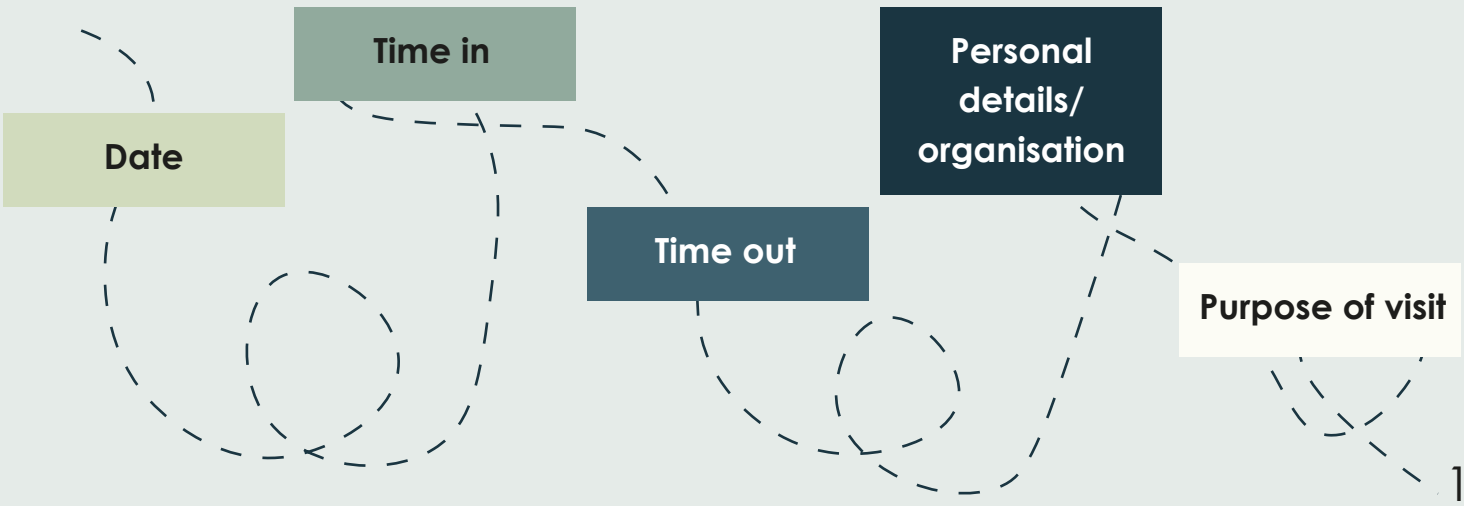
The current CCTV Maintenance and repair contractor is:
Tendring Telecoms & Security Systems
11 Crusader Business Park
Stephenson Road West
Clacton-on-Sea
Essex
CO15 4TN01255 423345
info@ttss.org.uk

INCIDENT LOG - HANDOVER

The purpose of this is to advise operators on the following shift of on-going incidents and other matters of interest. All ongoing incidents should be passed to the next shift.

VISITORS LOG – CONTROL CENTRE

All visitors to the Control Centre will be required to complete their details in the Visitors Log. This log will contain the following details:-



OPERATING REQUIREMENTS FOR CCTV OPERATORS – GENERAL

TRAINING OF CCTV OPERATORS

Staff operating the system will not be allowed to do so until they have received training on how the system works. *They will be required to take and pass an assessment test of their ability and knowledge of the system, including the Codes of Practice and Operating Procedures.*

The integrity of the system and any subsequent evidence may be compromised if these standards are not met. (This training will take place after they commence employment).

When new or updated equipment is installed in the Control Centre, operators are to be trained in its operation and use by the installers.

MONITORING THE CAMERAS – CONTROL CENTRE

The Control Centre is operational 24 hours per day, every day of the year. A minimum of two Operators are to be on duty at any time.

The basic functions of the Control Centre Operator are to operate the CCTV, Careline and out-of-hours systems connected to the Control Centre. This includes: the CCTV cameras, car park access gates and Council out-of-hours telephone. Off-going CCTV Operators will ensure that they fully brief any on-coming Operators as to any noteworthy or ongoing incidents for that day.

CCTV Operators will have to perform a number of functions other than surveillance and Operators will not be expected to sit at the workstation constantly throughout their shift.

A general health and safety recommendation is that the Operator's do not view screens for continuous periods. Operators receive a 15 minute break during their shift. They should remain available to respond when an incident occurs or respond to the telephone.

If two Operators are on duty, they must ensure that one Operator is present in the Control Centre at all times.

When monitoring the cameras, CCTV Operators will be expected to take the lead role in their use. They should be familiar with all the streets and areas covered including likely areas of criminal activity and known trouble spots. They should maintain a working relationship with the Police Officers patrolling the streets as and in addition, it will be essential to maintain contact with other staff together with any other agencies involved in a particular incident.

In the event of a major incident or authorised pre-planned operation and any other agreed condition as long as it is in accordance with the scheme aims, the police may take control of the Control Centre. Assignation of control of the system may be requested only by a Police Officer of the rank of Chief Inspector or higher and granted by a member of Authorised Staff.

When appropriate, liaison with the local police, in particular, the Police town centre Neighbourhood team should be made to improve the CCTV Operators' knowledge of local known criminals.

MONITORING THE CAMERAS – STAND-ALONE SYSTEMS

These cameras are generally not monitored in real time. Typically they will only be used when staff become aware of an incident in progress, or after it an incident has happed for review purposes.

USE OF PERSONAL DATA FROM ESSEX POLICE

Under Data Protection Act legislation Essex Police has an obligation to ensure that both Essex Police and Tendring District Council staff treat 'Police owned' personal data appropriately.

From time to time Essex Police may share information of a personal nature with Control Centre staff (photos, name, description etc.). This date is to be treated under GDPR rules and regulations. It should not be shared outside of the Control Centre. All data should be destroyed when any investigations are concluded.

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

From time to time, the Police or other statutory investigating agency will make a request to view certain areas or people in order to carry out targeted surveillance. Where this request is for pre-planned operation, CCTV Operators must ensure that the required authority authorising surveillance under the Regulation of Investigatory Powers Act (RIPA) has been granted and that the front page of the authority is issued to the Council showing the extent of the authority.

It is essential that CCTV Operators are aware of this requirement and as such forms part of the training package. Generally it is the Police that request such surveillance but other investigative agencies could make use of the CCTV system (e.g. Customs & Excise, other Government Departments). Only agencies with prosecution powers may be permitted to use the CCTV System in accordance with the Codes of Practice.

RIPA forms exist for Tendring District Council 'in house' pre planned operations (Trading Standards etc.) and CCTV Operators should ensure they have been authorised before surveillance commences. Authorisation is not required if the surveillance required is an immediate response to events found by normal patrolling, either by Police Officers, store Security Officers or by CCTV Operators.

ACTION WHEN A CCTV OPERATOR OBSERVES AN INCIDENT OR IS INFORMED OF AN INCIDENT.

When a CCTV Operator observes an incident they should try to obtain the best available pictures of the area concerned. This should be done by using adjacent cameras to view the relevant target area. It may be appropriate for a second camera Operator to take over any other incidents allowing the main Operator to concentrate on the current incident. Any incident viewed on the 'spot' monitor is displayed on the Police monitor in Clacton Police Station. It may be appropriate that the Police then assume control of that or any other camera, albeit with the concurrence of the Control Centre Operator.

The CCTV Operator should continue to monitor activity with the aim of producing the best available pictures. This will include zooming in to record close up facial images and registration numbers of vehicles. The Operators must at this point work closely with the Police and if necessary, assist with advice on deployment of Police Officers to the incident location.

It may be necessary for the CCTV Operator to speak directly to outside staff and give directions. This should be done in conjunction with the Police dispatcher. The CCTV Operator will continue to monitor the Police Officer and subject on camera for as long as possible, this being particularly important when an arrest is made. This enhances Police Officer safety and obtains the best evidential pictures for the court.

The responsibility for the overall control of any incident remains with the Police Officers at the scene. When an incident has finished the Incident Log must be completed with all relevant facts as previously described.

ACTION WHEN THE ALARM INTERFACE ACTIVATES

The systems do not have an alarm interface.

ACTION WHEN ANPR (AUTOMATIC NUMBER PLATE RECOGNITION) ALARM ACTIVATES

Data from the Police ANPR cameras are not received by the CCTV Control Centre. Currently there are no ANPR cameras on the CCTV system

ACTION WHEN FACIAL RECOGNITION ALARM ACTIVATES

There is no Facial Recognition software nor alarms connected to the CCTV system.

ACTION – SLOW TIME (CONTROL CENTRE)

There will be many occasions when no incidents or suspicious activity is seen on camera. At such times, the CCTV Operator should use the opportunity to patrol the area in an attempt to prevent and detect crime and increase the general feeling of safety. This may also involve the use of pre-set facilities and also the sequencing facility that will set the cameras into an automatic patrol.

The CCTV Operator should be aware that the CCTV Control Centre functions extend beyond crime fighting and on occasions the cameras will be queried to assist the public e.g. looking for lost children, wandering adults with dementia etc. These functions, although not primary functions, assist with the credibility of the CCTV system.

There may be other uses for the CCTV made in agreement with the other agencies and by way of local agreement. They will at all times be in accordance with the Code of Practice. The CCTV System enables Police to view a slave monitor positioned at Clacton Police Station. The Code of Practice applies to this location in respect of access to viewing and recording. It is a legal requirement under the Data Protection Act 1998 that access to these images is controlled accordingly.

USE OF THE SYSTEM BY OUTSIDE AGENCIES

In all cases the use of the CCTV system must comply with the Tendring District Council CCTV Code of Practice and all statutory regulations including the Data Protection Act, Human Rights Act, Regulation of Investigatory Powers Act and Protection of Freedoms Act.

Only agencies with prosecution powers may be permitted to use the system in accordance with the Codes of Practice. As a rule, use of the systems by external agencies is to be pre-arranged. In cases where an immediate need is apparent, permission should be sought and granted by a member of Authorised Staff. She/he will make a judgment based on the intended use by the particular agency concerned. Tendring District Council employees will retain operation and control of the Control Centre systems but with the direction of the external agency.

COMPLAINTS PROCEDURE

Complaints about the service are to be made following the Council's existing complaints procedure, see Council website http://www.tendringdc.gov.uk/council/consultation-contact-and-complaints/how-complain

CRIME INVESTIGATION AND PROSECUTION PROCEDURES

Action to be taken relating to crime investigations and prosecution with regard to data recordings and statements for use as information and evidence relating to a specific incident.

POST-INCIDENT VIEWING OF RECORDED IMAGES

After an incident has taken place a Police Officer may wish to view the recorded data to establish if relevant material exists. If no evidential material is found, then the reviewed material on the DVR or other appropriate media must be dealt with in accordance with Criminal Proceedings and Investigation Act (CPIA). Under normal operating conditions, the digital images will be retained for 30 days before being automatically deleted. It is essential therefore that a Police Officer reviews recorded images within that period otherwise evidential material will be lost.

A review station is located in the Control Centre and at other stand-alone sites for use by the Control Centre staff and other authorised agencies to review and download images, but this must only be carried out under the supervision of the Control Centre staff.

Police. - Appointments may be made with the CCTV Control Centre staff (or authorised staff at the stand-alone sites) before attending to conduct a review. Due to the technical nature of the equipment CCTV Operators may assist Police Officers with the review but will not carry out lengthy searches for them. Operators may need to interrogate the system on behalf of the investigating police officer, but lengthy and time consuming sessions will be the responsibility of the Police officer and they should set aside sufficient time to do so.

RECORDINGS

All cameras are recorded and images retained for 30 days. *Following an incident the CCTV Operator will ensure that the Police are notified at an early opportunity. It may be necessary for Police Officers to view this material prior to starting interviews etc. and they should request to do so as soon as they become aware of the material being available. It is vital that the Incident Log contains sufficient details of the incident to link up the data stored. The Log should indicate that footage exists.*

HARD COPY OR PHOTO IMAGES

This system has the ability to produce hard copy or video stills from recorded images. These photographic images are data in the same way as video images and must be controlled in the same way. A full record of photographs or prints produced by the CCTV System must be maintained. Where photographs or prints are removed from the Control Centre, full details must be recorded in the Viewing and Copying Log.

STATEMENTS

Section 72(1) Police and Criminal Evidence Act 1984 holds that a statement has the same meaning as in part 1 of the Civil Evidence Act 1968. Section 10 of that act holds that a 'statement' includes any representation of fact whether made in words or otherwise and includes film, negative, tape or other device by which visual images may be produced. An (evidential) digital recording must therefore be regarded as a document within the terms of the Police and Criminal Evidence Act 1984.

In any court proceedings the evidence of witnesses must be prepared as if video evidence does not exist and therefore be complete and descriptive. The video images will be produced as evidence having been exhibited as with any other form of documentary exhibit. In effect this means that statements may be taken from CCTV Operators detailing what was seen of an event as if the Operator was present at the scene. On occasion, statements may also be required to prove the integrity and audit trail of the data.

CRIMINAL PROCEDURES AND INVESTIGATIONS ACT 1996 (CPIA)

A resume of the CPIA as far as it may be applicable to the gathering, recording and retention of evidence by CCTV systems is attached as Appendix A. It is imperative that CCTV Operators comply strictly with the Act at all times.

VIEWING AND COPYING PROCEDURES/VIEWING RECORDED IMAGES

In a recent court case, it was directed that Police Officers must view evidence of recorded images and provide continuity, and not solely the CCTV Operator. This process must be followed in order not to step outside of these guidelines and rules of evidence.

REVIEW OF RECORDED IMAGES

It will be the responsibility of the Officer in charge (OIC) to enquire with the CCTV Operator whether evidence is available or not. The Operator may assist the Police Officer in the operation of the viewing equipment but will not be expected to view the images on their behalf for long periods of time. In some circumstances the Operators may view the images and inform the Police Officers of the validity of evidence available, the Police Officer will then be invited to view the images themselves. If the request is for long periods of time, then Police Officers will be invited to do the initial viewing themselves. A Viewing Suite is available at the Control Centre. All viewing must be carried out in connection with the aims of the CCTV system. In addition the review equipment may be used for training and demonstration purposes. This data is confidential material and the Data Protection Act applies.

DIGITAL STORAGE SYSTEM

Police Officers should note that the type of recording available is in digital format. In order to secure evidence, Police Officers should apply to a member of Authorised Staff or a CCTV Operator for either:

Once evidence has been identified, it will be copied to recordable media – Digital versatile Disk (DVD), USB Drive, or Hard Disk Drive (HDD) and handed to the officer. The Viewing and Copying Log must be clearly identified as such. The Viewing and Copying Log will be fully completed at the time of copying. It is not necessary to make additional copies for storage at the CCTV Control Centre.

CCTV OPERATING PROCEDURES

The Chief Executive of Tendring District Council is the Data Controller for the purposes of the Data Protection Act 2018 and the Council retains copyright of all recorded images leaving the Control Centre and other stand-alone sites. However once an image has been disclosed to another body, such as the police, the recipient becomes responsible for that image. It is the recipient's responsibility to comply with any other legal obligations such as the General Data Protection Regulation (GDPR) in relation to further disclosures. This ensures that copies which may be handed lawfully to Solicitors, are not used in the media without due regard to the ownership. Essex Police is entitled to make further copies of images in their possession and obtained from the CCTV System in pursuit of lawful investigation and in accordance with prevailing legislation. If further copies of the images are required, then they will be made in accordance with local Essex Police procedure but from the disclosed images, the DVD or other. Generally further copies will be produced by Essex Police themselves in accordance with its procedures and in compliance with Copyright terms.

Note - it is acceptable to copy more than one event into a single working copy for ease of viewing. Generally, it is best to create a composite recording with footage in a chronological manner, which has been shown to assist the courts with presentation of evidence. For copying, it is recommended that the operator record at least 2 minutes before and after the relevant footage to show no tampering has been carried out with the images. The copies will require statements to prove a fully documented audit trail, as well as helping to prove their integrity. Police Officers are not to remove any of the recordings from the CCTV Control Centre or other stand-alone sites without authority from a member of Authorised Staff or CCTV Operator.

Tendring District Council will rely on Primary, Alternate, Contingency and Emergency (PACE) Code of Practice 'B' para 6.5 where any request is made to seize the DVR Hard Drive. (Where an Officer considers that a computer may contain information, which could be used as evidence, he may require the information to be produced in a form, which can be taken away and in which it is visible and legible).

VIDEO STILL COPY - PROCEDURES

Use of the video printer or other hard copy equipment to produce video stills (photographic prints) shall be restricted to occasions when such prints will assist in fulfilling the objectives of the CCTV system, particularly in aiding identification of persons. Use in training and for demonstration is accepted. A log will be maintained regardless of the reason for which the prints were taken. This is incorporated in the CCTV Creation log. The person removing will sign the log to acknowledge receipt of and responsibility for the print. A print can only be removed from the CCTV Control Centre by a Police Officer or member of a statutory investigation agency. In all cases Tendring District Council retains Copyright © on these prints as detailed above. Given the importance of video evidence, great care should be taken to comply with all requirements of this aspect of digital tape management. Any shortcomings will also bring into question the credibility of the overall CCTV System.

ACCESS BY DATA SUBJECTS – SUBJECT ACCESS REQUESTS (SARS)

All staff must be able to recognise a request for access to recorded images by data subjects, (sixth and seventh Data Protection principle). Data subject requests mostly come via the single gateway approach into the Corporate Team and are then forwarded to the Information Governance and IT Manager to process. All SARs will be provided with a Standard Subject Access Request Form (Form SARF) that:-

Indicates the information required to locate the images requested

Indicates the information required to identify the person making the request

Asks whether the individual would be satisfied with merely viewing the images recorded.

Indicates that a response will be made promptly and no longer than 40 days from the day the request was received (which will be endorsed on the form).

Individuals will be provided with a description and purpose of images recorded and retained and provided with information about the disclosure policy in relation to those images (sixth Data Protection principle). When an agreement has been made to release the data, a member of Authorised Staff or designated member of staff may deal with the subject access request. As part of the Data Subject Access process, checks will be made with the appropriate authorities to ensure that any disclosure would not prejudice the prevention/detection of crime, apprehension/prosecution of offenders. Where the individual is seeking access to 'Essex Police owned' data or data which could be considered jointly owned then Tendring District Council should liaise with the Subject Access Administrator, Essex Police Headquarters.

FREEDOM OF INFORMATION REQUESTS

The Freedom of Information Act 2000 ("the FOIA") gives the public extensive rights of access to information held by the Council. FOIA requests are to be made via the online form on the Council's website, see https://www.tendringdc.gov.uk/council/your-right-know/data-protection-privacy-notice-and-cookies/freedom-information-and-eir

All requests must be dealt with in accordance with the procedure and must not be dealt with directly by the Control Centre. Any requests received by the Control Centre are to be forwarded immediately to the Council's Information Governance and IT Manager.

RECORDED IMAGES MANAGEMENT

RETENTION POLICY

All downloaded (burnt) images and written records that may be relevant to an investigation must be retained for 6 months.

EMERGENCY PROCEDURES

If the need arises to evacuate the Control Centre or other stand-alone site by virtue of a security alert or fire alarm, all staff will act in accordance with local instructions.

If possible but without risking the safety of any member of staff, the Control Centre or stand-alone site should be secured on leaving. Any operations or procedures under way at the time of evacuation should be abandoned.

On returning to the Control Centre or stand-alone site all systems should be checked to ensure they are in full working order. An appropriate entry should be made in the Incident Log noting relevant times, alarm type and action taken.

IDENTIFICATION PROCEDURES USING RECORDED IMAGES PACE CODES OF PRACTICE

The overriding principle governing all identification procedures is that Police Officers must comply with the Police and Criminal Evidence Act 1984 and associated Codes of Practice, (Particularly Code D and relevant annexes).

INTEGRITY OF STORAGE OF RECORDED IMAGES

Where recorded evidence is available, the protection of that evidence is of paramount importance. Data security must comply with these operating procedures at all times. If for any reason a data medium cannot be processed accordingly a member of Authorised Staff must be informed without delay.

ACCEPTABLE VIEWING OF IMAGES

An investigating Officer may show a video images or photographs (video stills) of an incident to the public using the local or national media to assist in the recognition and tracing of suspects. The PACE Code of Practice sets out the guidelines in this area.

IDENTIFICATION WHERE A SUSPECT IS NOT KNOWN AND THE INCIDENT FILMED.

Referring to the cases of R v Jones, it is considered permissible to show images that may contain the incident even though it has been obtained several days or weeks after the incident. Refer to PACE Codes of Practice, Code D, Para 2.21a which states. 'Nothing in this code inhibits an investigating officer from showing a video film of an incident to the public at large through the national, or local media, or to Police Officers, for the purposes of recognition and tracing suspects. However when such material is shown to potential witnesses (including Police Officers) for the purpose of obtaining evidence, it shall be shown on an individual basis so as to avoid any possibility of collusion, and the showing shall, as far as possible, follow the principles of Video Film Identification (Para 2.10) or Identification by Photographs (Para 2.18)

SHOWING RECORDED IMAGES TO A SUSPECT

It is considered permissible to show recorded images to a suspect if this would assist the investigation. In many cases, the evidence recorded will support the prosecution case and shorten the amount of enquiries required.

DEVELOPMENT OF CCTV SYSTEM

THE CCTV SYSTEM DEVELOPMENT – ENVIRONMENTAL

The CCTV System will continue to develop according to the needs of the Local Authority and any Partnerships, taking into account the environmental issues affecting it e.g. buildings and street furniture obscuring cameras etc.

CCTV SYSTEM DEVELOPMENT – TECHNICAL

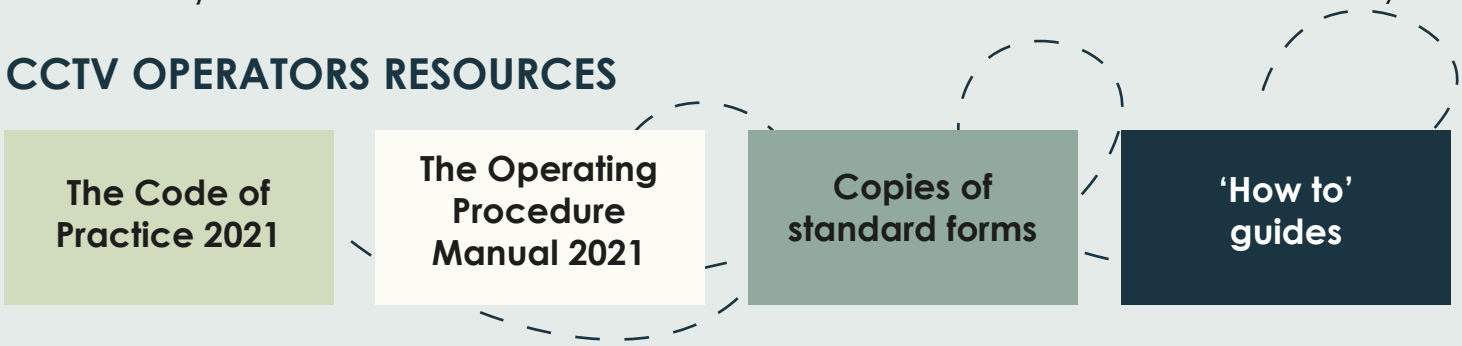
The CCTV System may be enhanced in the future by the supply of additional cameras or facilities according to needs identified by the Local Authority or any Partners. Improvements and additions may take place taking into account technological advancement.

CCTV BEST VALUE

The CCTV system will be regularly reviewed and upgraded where budgets allow, taking into consideration 'best value' in terms of detection, prevention and prosecution of crime.

A representative from the CCTV Control Centre will regularly attend the Community Safety Partnership Group meetings and other relevant groups (such as PubWatch) in order to understand the needs to the local business community.

CCTV OPERATORS RESOURCES



UPDATING CCTV OPERATING PROCEDURES MANUAL

These operating procedures are subject to continuous update. A breach of any aspect of this Operating Manual or the Code of Practice may involve disciplinary action in accordance with Tendring District Council 'Formal Discipline Code' and may result in dismissal, which may not be preceded by a warning.

APPENDIX A

THE CRIMINAL PROCEDURES AND INVESTIGATIONS ACT 1996 (CPIA)

CPIA came into effect on 1st April 1997 and introduced a statutory framework for the disclosure to defendants of material, which the prosecution would not intend to use in the presentation of its own case, (known as unused material).
The Act introduced some changes, which will have an impact upon how investigating Police Officers gather and deal with potential evidence which, in turn will almost certainly impact on CCTV systems. The three key words are **Record, Retain, Reveal.** The first two will have a bearing on CCTV systems and procedures need to be in place to ensure compliance with the requirements of this Act.

RECORD

WHEN AND HOW SHOULD MATERIAL BE RECORDED?

"Information should be recorded at the time it is obtained or as soon as practicable after that. Material should be recorded in a durable or retrievable form …..".

RETAIN

WHAT MATERIAL SHOULD BE RETAINED?

"*All material, including information (which would include that recorded by way of video tapes / digital storage system) and objects, which is* ***obtained in the course of*** *a criminal investigation and which* ***may be relevant to the investigation***".

WHAT IS THE TEST FOR RELEVANCE?

"*Material* ***may be relevant to the investigation*** *if it appears to have some bearing on any offence under investigation or any person being investigated, or to the surrounding circumstances of the case* ***unless it is incapable of having any impact on the case"***

REVEAL

Responsibility for the revelation of material rests with the Disclosure Officer, who may also be the Investigating Officer.

THE TEST FOR DISCLOSURE

"…..any prosecution material which has not previously been disclosed to the accused and which in the prosecutor's ***opinion might undermine the prosecution against the accused"***

RESPONSIBILITIES

In conducting an investigation, the investigator should pursue all reasonable lines of enquiry, whether these point towards or away from the suspect. What is reasonable in each case will depend on the particular circumstances. There is now an onus upon the investigator to ensure that all potential evidence is retained. In view of the requirement to record information at the time it is obtained or as soon as is practicable afterwards in a durable and retrievable form CCTV Operators are likely to find themselves making more written records that prior to the introduction of the Act. This is especially relevant to the description of people, vehicles and events. Any written records are likely to become disclosable. This is particularly important when suspect descriptions are recorded in the Operator Log, as this is likely to be the place where these descriptions are recorded in the Operator Log, as this is likely to be the place where these descriptions are FIRST recorded. (The defence are entitled to this as a matter of routine). Any request from a Police Officer to conduct a search for an event or suspect which produces a negative result in the sense that these items were not found, may still be relevant to the defendant at a later stage of the enquiry. For this reason a copy of the searched data should be recorded to whatever format the Police Officer requires.