Dover District Council

CCTV POLICY STATEMENT

December 2015

DOVER DISTRICT COUNCIL - CCTV POLICY

1. Introduction

1.1 Dover District Council (DDC) uses Closed Circuit Television (CCTV) systems in public spaces, within car parks and at a number of the organisation's owned sites.

1.2 This document along with individual systems Codes of Practice are designed to give clear guidelines on DDC's use of CCTV and to protect the organisation and its CCTV operators from allegations of misuse of the system and to protect staff and the public from any abuse of the CCTV system.

1.3 This policy covers the purchase and use of CCTV equipment and the gathering, storage, use and disposal of visual data. This policy applies to all staff employed by DDC and should be the standard expected from any external agencies or persons who operate CCTV systems on its behalf.

1.4 This document should be read in conjunction with the CCTV systems Code of Practice and Operational Manual. Failure to comply with these documents could lead to disciplinary action, which may lead to dismissal and in certain circumstances criminal proceedings against the individuals concerned.

2. Objectives of CCTV Systems

2.1 It is important that everyone and especially those charged with operating the CCTV systems on behalf of the Council understand exactly why each of the systems has been introduced and what the cameras will and will not be used for.

2.2 Each CCTV system will have its own site or task specific objectives. These will include some or all of the following:

- **Protecting areas and premises used by staff and the public;**
- **Deterring and detecting crime and anti-social behaviour;**
- **Assisting in the identification of offenders leading to their arrest and successful Prosecution or other appropriate action;**
- **Reducing violent or aggressive behaviour towards staff;**
- **Reducing fear of crime, anti-social behaviour and aggression;**
- **Protecting property and assets owned by Dover District Council;**
- **Assisting in staff disciplinary, grievance, formal complaints and Health and Safety Investigations.**

2.3 Individuals will only be monitored if there is reasonable cause to suspect that a criminal offence or serious breach of discipline (potentially amounting to misconduct) has been, or may be about to be committed. This will only be permitted when authorised and may require the use of a RIPA authorisation. The Responsible Officer should consult the Heads of Legal Services and Human Resources before any such action is taken.

3. Legislation

3.1 In addition to DDC's policies, procedures, guidelines and Codes of Practice, CCTV and its operation are subject to legislation under:

3.1.1 The Data Protection Act 1998 (DPA).

3.1.2 The Human Rights Act 1998 (HRA).

3.1.3 The Freedom of Information Act 2000 (FOIA).

3.1.4 The Regulation of Investigatory Powers Act 2000 (RIPA).

3.1.5 The Protection of Freedoms Act 2012.

3.2 It is important that the operation of all the DDC run CCTV systems comply with these Acts, policies, procedures, guidelines and Codes of Practice. This is to ensure that staff running the CCTV systems, the public and the Council itself are protected from abuses of the CCTV systems. The Responsible Officer will be responsible for reviewing all CCTV documentation relating to their system annually (or as changes occur) and ensuring the information in those documents is up to date**.** The CCTV Manager who acts as the Single Point of Contact (SPOC) will assist in this process.

4. The Responsible Officer

Is responsible for:

4.1 The day-to-day operation of the CCTV system within their charge and the security and accountability of all equipment and media used by their system. This includes any system owned by DDC but which is in the possession of third parties such as those cameras deployed in shopping precincts, commercial properties and swimming pools.

4.2 Making sure that authorised staff (the Responsible Officer, their operating team, the CCTV Manager and people authorised to view images) using the CCTV system are properly trained in the use of the equipment and comply with the Code of Practice and policies and procedures. They are not to permit any other staff to operate the equipment or view images without authorisation.

4.3 Acting as the first point of contact for enquires, complaints and requests for evidence and as the liaison officer for all external and internal contacts.

4.4 The Responsible Officer may delegate aspects of this role, as appropriate, but will remain accountable.

4.5 The Responsible Officer nor their staff will not instigate a RIPA request on their own behalf.

4.6 The SPOC will be responsible for ensuring all users are kept up to date on legislation and changes in procedures and will review DDC's Policy and Codes of Practice documents annually, and maintain a central database of all documents relating to the Council's CCTV system

4.1 CCTV Staff Operating CCTV Systems

4.1.1 Staff operating CCTV systems are responsible for operating the equipment in accordance with requirements set out in current legislation, this policy document, guidelines, confidentiality certificates, Codes of Practice and local Operational Manuals.

4.1.2 They must ensure that their training is up to date.

4.1.3 They are responsible for bringing any faults or misuse of the equipment to the Responsible Officer's attention immediately.

5. Purchase and Deployment of CCTV Cameras

5.1 DDC is committed to respecting people's rights to privacy and supports the individual's entitlement to go about their lawful business. This is a primary consideration in the operation of any CCTV system, although there will inevitably be some loss of privacy when CCTV cameras are installed.

5.2 Therefore it is crucial that serious consideration is given to the necessity for cameras in a given location, and their impact on the privacy of individuals using the areas where cameras are to be installed.

5.3 Cameras are not to be installed in such a way that they can look into private space such as houses. If cameras are required in these areas they must only be installed if they can be fitted with privacy zones, which block out private areas so that they cannot be viewed or recorded**.**

5.4 Covert cameras are not normally to be deployed into areas used by staff or the public. Cameras should normally be clearly visible and clearly signed.

5.5 Concealed and unsigned cameras within property may on rare occasions be deployed in areas of high security where there is no legitimate public access and where staff access is controlled and restricted. Staff who normally work in these areas should where appropriate be informed of the location of these cameras, their purpose and where the monitor is kept.

5.6 It is a requirement under the Information Commissioners Code of Practice and the National CCTV Strategy that any equipment purchased is fit for purpose and will meet the objectives set down for the scheme. There is also a clear requirement for all CCTV schemes to have an effective maintenance schedule and Code of Practice. Officer's purchasing new CCTV equipment need to ensure these requirements are met.

5.7 This Council does not deploy 'Dummy' cameras as these give a false sense of security. Neither are officers to purchase cameras that can monitor conversation or be used to talk to individuals as this is seen as an unnecessary invasion of privacy.

5.8 Once new cameras have been installed a copy of a map or building plan showing the location of the CCTV cameras should be sent to the SPOC for inclusion in the central CCTV library.

6. Monitoring

6.1 CCTV monitors sited in reception areas are intended to provide live monitoring of reception areas by Departments. It is the responsibility of the Responsible Officer in the Departments concerned to ensure those observing the monitors are properly trained in their duties and responsibilities and that the ability to view the monitors is restricted to those authorised to see it.

6.2 Monitoring of other cameras where required will only

7. Viewing Images and the Provision of Evidence

7.1 The casual viewing or trawling of images is strictly forbidden. Viewings must only be undertaken for a specific, legitimate purpose.

7.2 The provision of evidence or viewings will normally be requested either by the police, other enforcement agency or another department conducting an investigation into criminal activities, potential disciplinary matters, complaints, grievance or Health and Safety issues.

7.3 Enforcement agencies such as the police have a legal requirement to 'seize' any relevant evidence when investigating a crime and Responsible Officers must comply with their request. But the enforcement agencies are bound by the same rules as everyone else.

7.4 Enforcement agencies are not permitted to trawl the CCTV system on the off chance of detecting a crime or wrong doing. They are required to provide the Responsible Officer with a Crime or Incident number of other such proof that they are conducting a legitimate investigation.

7.5 The release of evidence or permission to view images may only be authorised by the Responsible Officer or in their absence, the Head of Service or the Departmental Director**.** Where an enforcement agency requests copies of an image, one copy is to be made but there is no requirement for the Responsible Officer to retain or produce any further copies.

7.6 If the matter concerns a member of staff, there will be no automatic right to viewing or the release of images. Viewings will be permitted and images will only be released to a properly authorised investigating officer after they have submitted a formal request to the Departmental Director.

7.7 The Responsible Officer will then hold the relevant footage on the computers hard drive (but not copy it to disc) and then seek authority to release the images from the Head of Service or Departmental Director. The Head of Human Resources and when appropriate the Head of Legal Services should also be consulted before the images are released to the Investigating Officer.

7.8 It is appreciated that this process may take a little time and officers should move quickly to complete the process so that the investigation is not unnecessarily delayed. To ensure the images are not lost due to retention time, the Investigating Officer can formally ask the Responsible Officer to retain the images until the viewing/ release of evidence process has been completed.

7.9 Once authorised, arrangements will be made to enable the Investigating Officer to view the images and if necessary be issued with two copies of recorded material on suitable recording media. Note: Only the Investigating Officer is permitted to view the images at this stage.

7.10 The reason for the second disc is that if it is decided to use CCTV images in an employment related hearing the person being investigated must be given a copy of the images to permit them and their representatives to mount a defence. At the end of the hearing ALL copies of the images are to be collected by HR, held on file and destroyed once the appeals process and any Employment Tribunal processes have been completed.

7.11 Staff who are subject to disciplinary, complaints or grievance procedures have the right to request that footage be retained if they believe it will support their defence. The process will be exactly the same as that shown above for the Investigating Officer.

7.12 **The Council will not permit viewings or release images to people being investigated by an enforcement agency or in an internal investigation, which may be handed over to an external agency such as the police.** The responsibility for investigating and disclosing images to those involved in the investigation are covered by the Police and Criminal Evidence Act (PACE) and the Evidence and Disclosure Act and the prosecuting authorities are required to follow the procedures set out in these Acts. It should be noted that other enforcement agencies will operate under other legislation but the use of and disclosure of the evidence rests with them.

7.14 It is critical that a full and detailed record is kept of all viewings of the systems and all instances when images are issued. This information must include:

- Date, time, camera number and location of the incident
- The name of the authorising officer
- The date time, name and contact details of the person viewing or removing images
- The reason for the viewing/ issue of images
- Details of the person who released and the received the images
- Any media containing images should be uniquely marked and the number recorded for ease of identification

8. Insurance Claims

8.1 CCTV involvement in insurance claims fall into two categories. Firstly, incidents which may result in claims against the Council and secondly claims involving third parties, normally traffic accidents.

8.2 CCTV cameras may be able to assist in incidents that could result in a claim against the Council**.** When a report is received which may result in a claim, the Officer responsible for dealing with the incident should consider whether CCTV covers the area. If so they should then ask the CCTV systems Responsible Officer to hold images for that period but this must be done within 28 days from the date of the incident. The

Officer dealing with the incident should then follow the procedures for viewing and obtaining evidence, which is set out in section 7 above.

8.3 If evidence is issued to the Officer dealing with the incident, they become responsible for the security, safety and integrity of the images. All recorded media must be stored in a secure place with access limited only to those people involved in the subsequent claim. At the end of the waiting period or after any claim has been dealt with this officer will be responsible for the destruction of the recorded media by shredding and a record in the form of a signed memo to that effect will be kept for a period of 12 months.

8.4 Requests for assistance from CCTV cameras in third party claims are increasing especially with regard to traffic accidents. Often it is the person involved in the accident who will contact CCTV and ask either if we have any images or if they can come and have a look. Requests of this kind should normally be refused. Instead, members of the public should be advised to contact their insurance company and ask them to write to the Responsible Officer formally, giving as much detail about the incident as possible and requesting assistance. It is also important that it is stressed to the person requesting the information that the letter is received before the overwrite period on the recorder. No other action should be taken at this stage.

8.5 If the letter arrives within the recording period, the Responsible Officer should view the images. If the incident was not caught on camera the insurers or solicitor can be called and informed and the case can be closed. If the letter arrives after the recording period, there will be no relevant images and again the person requesting the images should be informed.

8.6 If relevant images are found on the recorder, the insurance company/Solicitor should be informed and asked if they want a copy. If they do, then they need to be informed that there will be a fee. The fee is based on the amount of time spent by staff viewing, copying and processing the images based on the hourly salary rate (currently £17.50) rounded up to the nearest hour. It should also include post and packaging and the cost of the media supplied. This should then be sent as an invoice to the recipient. No charges will be raised against internal requests for assistance.

8.7 The images may then be copied and sent to the relevant person accompanied by two copies of a letter reminding them that the DDC retains ‘copyright’ over the images, that they are responsible for the security and destruction of the images and that the images may not be used for any other purpose other than the one they were released for. The details of the media released should be included (i.e. media number) in the letter and they should be asked to sign one copy of the letter confirming they have received the images and accepting the conditions of release. A detailed record of all actions must be maintained. Failure to comply with the conditions of release may result in legal action being taken against the person who signed the acceptance letter.

9. Signage

9.1 All areas where CCTV is in use should be clearly signed to comply with the Data Protection Act. This is to warn people that they are about to enter an area covered by CCTV cameras or to remind them that they are still in an area covered by CCTV. The signs will also act as an additional deterrent. CCTV signs should not be displayed in areas, which do not have CCTV cameras.

9.2 Where ‘Covert’ cameras have been authorised for deployment, signage will not normally be erected.

9.3 The sign should carry the CCTV camera and DDC's Logo. The information on the sign should explain why the CCTV cameras are there, who runs them and a contact number. The signs, position and the message needs to be big enough to enable people to easily read the information on it. For pedestrians the sign should be A4 size and for vehicle access A3 size.

10. Third Party Access Requests

10.1 Under the Data Protection Act and the Freedom of Information Act members of the public and other organisations have the right to ask to see data held by Local Authorities and other Public Bodies. This data includes visual images captured by CCTV.

10.2 As a general principle access to this data should not be refused. However there are certain circumstances when it will not be possible to provide images from CCTV - for example, when the images form part of a criminal investigation. In all instances where Access Requests are received, they should be passed onto the DDC's Data Access Request Officer (who has responsibility for dealing with Access Requests) for action, before CCTV images are released.

11. Recording Systems

11.1 All staff required to operate CCTV equipment are to receive training in the use of the equipment and must conform to this Policy Document and their systems Code of Practice at all times. Staff who operate the recorders will be required to sign a 'Confidentiality Statement', which prohibits them from making any material available for purposes other than those stated in the Code of Practice. Any other staff having access to the equipment will also sign a Confidentiality Statement. Once signed, the Confidentiality Statement should be placed in the person's Personal file.

11.2 Except for evidential purposes images will not be copied in whole or in part.

11.3 Recorded material will not be sold or used for commercial purposes or the provision of entertainment. Images provided to the Police or other enforcement agencies or for internal investigations shall at no time be used for anything other than the purposes for which they were originally released.

11.4 Recording equipment and recording media will be kept in a secure location and no access will be granted to unauthorised staff.

11.5 All images will remain the property and copyright of the Council.

11.6 Each new recording media must be clearly marked with a unique reference number in indelible ink before it is brought into operation.

11.7 Each use of media will be noted in the CCTV Register. Unused media or media awaiting issue will be held in a secure cabinet in such a way that completeness of the archive is immediately apparent. The CCTV Register will be stored in a secure place.

11.8 All media will be disposed of securely when no longer required.

11.9 All recording protocol should be an 'Open' protocol. This enables the police and other agencies to view evidence on their own systems without having to preload operating software. This is important because most police computers are unable to download unauthorised software, which means they will be unable to use the CCTV images for their investigations.

12. Disciplinary Offences and Security

12.1 Tampering with or misuse of cameras, monitoring or recording equipment, images or recorded data by staff may be regarded as misconduct and could lead to disciplinary action, which may result in dismissal or criminal prosecution.

12.2 Any breach of this Policy Document or the CCTV Code of Practice will be regarded as a serious matter. Staff who are in breach of this instructions will be dealt with according to the DDC's disciplinary procedures.

12.3 The responsibility for guaranteeing the security and proper use of the system will rest with the Responsible Officer of the system concerned. These officers will, in the first instance, investigate all breaches or allegations of breaches of security or misuse and will report his/her findings their Director.

13. Statistics

13.1 CCTV installation like any other purchase by a Public Body is spending public money and this needs to be justified. CCTV systems are required to show how effective the cameras are in dealing with the objectives set out for them.

13.2 Responsible Officers will be required to submit an annual set of statistics showing the effectiveness of their systems to their Head of Service with a copy being sent to the SPOC. The statistics will cover the previous financial year (1st April – 31st March).

14. Inspections/ Visits

14.1 All CCTV system may be subject to inspections or visits by a member of the Information Commissioners Office or the Regulation of Investigatory Powers Commissioner. In addition, systems may also be subject to visits/ inspections by members of the organisation and the SPOC.

14.2 These visits/ inspections are designed purely to ensure that the systems are being run in accordance with current legislation, this Policy Guideline and their own Codes of Practice and to offer advice for improvement where required.

15. Health and Safety

15.1 The Responsible Officer is to ensure that staff are made aware of and comply with all the Council's policies on Health and Safety. In particular they are to be aware of policies relating to working with electrical equipment, VDU Regulations.

16. Complaints

16.1 Complaints about the operation of a CCTV system should be addressed initially to the Departmental Director. Complaints will be dealt with in accordance with DDC's complaints procedure.

17. Further Advice/ Information

17.1 Further advice on CCTV related matters may be obtained from the Head of Community Services.

Annexes:

A: Operational Assessment Form.
B: Privacy Impact Assessment Form.

Annex 'A' to the CCTV Policy
Dated December 2015

Operational Requirements Review

CCTV System:_____ **Responsible Officer:**_____

Ser	Operational Requirements	Requirements Met/ Comments
01	What was the original reason for installing a CCTV system? Is it still relevant?	
02	What are the current CCTV systems Objectives?	
03	Are the camera locations suitable for the task and do light levels or environmental issues such as tree growth affect them? (see attached Sheet)	
04	Can the cameras produce good quality images on an 'open protocol' which can be used in court and is the monitor of a high enough quality to view images?	
05	Are the cameras secure and protected from vandalism?	
06	Is the recording equipment and media in a secure area? Is access to this equipment and CCTV images restricted?	
07	Is the recording equipment of good quality and a storage capacity to ensure images are not corrupted and can be stored for a specified period of time?	
08	Are there regular function checks to ensure all equipment is operating and recording correctly and that all images are stamped with the correct date /time?	
09	Is there a comprehensive maintenance and cleaning regime in place?	
10	Do you have appropriate and sufficient signage in place to warn people that CCTV is in use?	
11	Is your Code of Practice on display so that members of staff and the public can read it?	
12	Are audits carried out regularly to ensure the security of all equipment and media and is a record of the audits kept for inspection? Are all media movements, viewings and evidence issues recorded?	

To be completed annually. One copy retained by the systems owner and a second copy sent to the SPOC by the 1st May.
Additional Notes:
Name of Inspecting Officer:_____ **Signature**:_____ **Date**:_____

(Location):_____

By Camera

Cam No	Date of Inst	Location	Arcs of Observation	Operational Task	Comments	Recommendations

Annex 'B' to CCTV Policy Statement
Dated December 2015

CCTV Privacy Impact Assessment Form

This form establishes the impact of CCTV on people's privacy and should be used to assess whether CCTV is justified and how it should be operated in practice. Once completed it should be reviewed annually. Copy to be sent to the Council's SPOC annually in May.

Ser	Issues to be considered	Results of assessment
01	Who will be using CCTV Images? Who will be legally responsible under the DPA?	
02	Why do you need CCTV? What problems it is meant to address? What other solutions to the problems were investigated and why have they been rejected?	
03	What are benefits to be gained by using CCTV?	
04	Can CCTV realistically deliver these benefits?	
05	Do you need to identify individuals or can you use a scheme not capable of identifying individuals?	
06	Can the system deliver the benefits now and in the future?	
07	What future demands will arise for wider use of the images and how will you cope?	
08	What are the views of those who will be under surveillance?	
09	How can you minimise intrusion of those who may monitored if specific concerns have been raised.	
10	Is the system established on a proper legal basis and operated within the law: DPA, HRA, RIPA and FOIA?	
11	Is the system necessary to address a pressing need, such as public safety, crime prevention, ASB or national security? If so what is the pressing need?	
12	Is the system justified in the circumstances?	
13	Is it proportionate to the problem it is designed to deal with?	
14	How has the capital and revenue cost been resolved?	

Over All Comments on Assessment:

Location of Scheme:_____

Name of Officer completing form:_____ **Signature**:_____ **Date**:_____