Dover District Council

CCTV Codes of Practice

CCTV UNIT DOVER DISTRICT COUNCIL

Dover District Council
1 February 2026

Table of Contents

Certificate of Agreement

The content of this Code of Practice is hereby approved in respect of Dover District Council's Public Space Surveillance System and, as far as is reasonably practicable, will be complied with by all who are involved in the management and operation of this system.

Signed for and on behalf of Dover District Council

Name: Nadeem AZIZ  **Position Held:** Chief Executive

Dated the 1st day of February 2026.

The completed authorised copy of this document is available to the public to view by contacting David Parratt, Community Safety, Resilience and Digital Manager, by email on David.Parratt@dover.gov.uk

Revision History

Version	Date	Summary of Changes	Initials	Changes Marked
1.0	01/02/2026	Introduction of new version control	DP	Changes of personnel, job roles and new design

Section 1 - Introduction and Objectives

1.1 Introduction

1.1.1 Dover District Council ('the Council') operates a Public Space Surveillance Closed Circuit Television system ('the System').

The System control room is located within the Dover District Council Offices at Whitfield and comprises of 107 cameras including 6 Automatic Number Plate Recognition (ANPR) Cameras.

Cameras are installed at strategic locations across the district. The majority of these cameras are fully operational with pan, tilt and zoom ('PTZ') functions, whilst others are fixed cameras.

There are no recording facilities at any location other than at the council offices at Whitfield. For the purpose of this document, the "owner" of the System is Dover District Council.

For the purposes of Data Protection Legislation, the Data Protection Act 2018, UK General Data Protection Regulation (GDPR) and Law Enforcement Processing (DPA18 Part 3) the 'data controller' is Dover District Council.

The Council manages the system.

Details of the owners of the system, together with their respective responsibilities are shown at Appendix A to this code.

1.2 Statement in respect of The Human Rights Act 1998

1.2.1 The Council recognises that public authorities and those organisations carrying out the functions of a public service are required to observe the obligations imposed by the Human Rights Act 1998. The Council considers that the use of the System in the district of Dover is a necessary, proportionate and suitable tool to help reduce crime and the fear of crime and to improve public safety.

1.2.2 Section 163 of the Criminal Justice and Public Order Act 1994 creates the power for local authorities to provide closed circuit television coverage of any land within their area for the purposes of crime prevention or victim welfare. Closed circuit television is also considered a necessary initiative by the Partners towards their duty under the Anti-social Behaviour, Crime and Policing Act 2014.

1.2.3 The Council also has power by virtue of its ownership and control of land and property to provide closed circuit television coverage of that land and property for the managements and security of that property and the activities carried on there, irrespective of whether or not the public are also permitted access to that land and property.

1.2.4 It is recognised that operation of the System has an impact on the privacy of individuals. The Council recognises its responsibility to ensure that the System should always comply with all relevant legislation to ensure its legality and legitimacy in a democratic society. The System will only be used as a proportionate response to identified problems. It will only be used in the interests of national security, public safety, the economic well-being of the area, the prevention and detection of crime or disorder, the protection of health and morals, or for the protection of the rights and freedoms of others.

1.2.5 Observance of this Code and the accompanying Procedure Manual shall ensure that evidence is secured, retained and made available as required with due regard to the rights of the individual.

1.2.6 The System shall be operated with respect for all individuals, recognising the individual right to be free from inhumane or degrading treatment and avoiding any form of discrimination on the basis of age, disability, gender, race, religion or belief, sexual orientation political or other opinion, national or social origin, association with a national minority, property, birth or other status.

1.3 Objectives of the System

1.3.1 The objectives of the System, which form the lawful basis for the processing of data, are:- -

- to help reduce the fear of crime and anti-social behaviour;
- to assist partner agencies to help those most at risk including but not limited to missing and vulnerable persons;
- to help deter crime;
- to help detect crime and provide evidential material for court proceedings;
- to provide assistance in the overall management of public health and safety;
- to enhance community safety, assist in developing the economic well-being of the Dover district and to encourage greater use of the town centres, shopping areas, car parks and similar locations within the district;
- to assist the Council in their enforcement and regulatory functions within the district of Dover.
- to assist the Council in the better management of its property assets to promote public safety, the economic well-being of the area, the prevention and detection of crime or disorder, the protection of health and morals, or for the protection of the rights and freedoms of others

1.3.2 Within this broad outline, the appropriate Divisional Commander of Kent Police, in partnership with the Chief Executive of Dover District Council, will periodically publish and review specific key objectives based on local concerns.

1.4 Procedural Manual

This Code is supplemented by a separate Procedure Manual, which provides guidelines on all aspects of the day-to-day operation of the System. To ensure the purpose and principles (see Section 2) of the System are realised, the Procedure Manual is based upon and expands the contents of this Code.

Section 2 - Statement of Purpose and Principles

2.1 Purpose

2.1.1. The purpose of this document is to state the intention of the Council, to support the objectives of the System and to outline how it is intended to do so.

The 'Purpose' of the system, and the process adopted in determining the 'reasons' for implementing the system are as previously defined, in order to achieve the objectives, set out within Section 1.

2.2 Guiding Principles

There are 12 guiding principles that System operators should adopt as listed below:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure it remains justified.
3. There must be as much transparency in the use of surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date[1].

1. Surveillance Camera Code of Practice (publishing.service.gov.uk)

2.3 Copyright

2.3.1. Copyright and ownership of all material recorded by virtue of the System will remain with the Council. Once an image or images has/have been disclosed to a partner such as the Police, then they become the Data Controller for the copy of that image(s). It is then the responsibility of that partner to comply with GDPR and the Data Protection Act 2018 in relation to any further disclosures.

2.4 Cameras and Area Coverage

2.4.1 The areas covered by the System are the public areas within the Dover district. These currently cover the towns of Dover, Deal, Sandwich, Aylesham and Wingham but may be expanded to cover any area within the boundaries of Dover District Council.

2.4.2 Transportable or mobile cameras may be temporarily sited within the District. The use of such cameras, and the data produced by virtue of their use, will always accord with the objectives of the System.

2.4.3 Most of the System cameras offer PTZ capability, which may automatically switch to monochrome in low light conditions.

2.4.4 None of the cameras forming part of the System will be installed in a covert manner. Some cameras may be enclosed within 'all weather domes', for aesthetic or operational reasons, but appropriate signs will identify the presence of all cameras.

2.4.5 Locations of all cameras within the System have been published on the Dover District Council website at https://www.dover.gov.uk/Community/Community-Safety/CCTV/CCTV-Locations.aspx (with the exception of cameras located upon or within land and buildings in the ownership and control of the Council and which are used solely to monitor activity within the confines of such land and buildings).

2.5 Monitoring and Recording Facilities

2.5.1 A staffed monitoring room, called the Control Room, is located within Dover District Councils Whitfield offices in Dover. The CCTV equipment installed there has the capability of recording all cameras simultaneously throughout every 24-hour period.

2.5.2 No equipment, other than that housed within the Control Room at Dover, shall be used for recording images from any camera forming part of the System for evidential purposes.

2.5.3 System operators are able to record images from selected cameras in real-time, produce hard copies of recorded images, replay or copy any pre-recorded data at their discretion and in accordance with the Code. Only trained and authorised users shall operate viewing and recording equipment..

2.6 Human Resources

2.6.1 Unauthorised persons will not have access to the Control Room without an authorised member of staff being present.

2.6.2 Operators, who are specially selected and trained in accordance with the strategy contained within the Procedure Manual, shall staff the Control Room.

2.6.3 All operators shall receive relevant training in the requirements of the Human Rights Act 1998, UK General Data Protection Regulations (GDPR), The Data Protection Act 2018, Regulation of Investigatory Powers Act 2000, this Code and the Procedure Manual. All staff will be licensed by the SIA. Further training will be identified and provided as necessary.

2.7 Processing and Handling Recorded Material

2.7.1 All recorded material, whether recorded in digital format, or as a hard copy video print, will be processed and handled strictly in accordance with this Code and the Procedure Manual.

2.8 Operators' Instructions

2.8.1 Technical instructions on the use of equipment housed within the Control Room are contained in a separate manual provided by the equipment suppliers.

2.9 Changes to the Code or the Procedural Manual

2.9.1 Any major changes to this Code or the Procedure Manual, i.e. changes that have a significant impact upon the Code or upon the operation of the System, will require consultation with and the agreement of all organisations with a participatory role in the operation of the System.

2.9.2 Minor changes may be required for clarification and which will not have a significant impact and will be included in the Code of Practice and the procedure manual without recourse to any partners.

Section 3 - Privacy and Data Protection

3.1 Public Concern

3.1.1 Although members of the public have become accustomed to the operation of CCTV and being observed, when concern is expressed, it is mainly over matters pertaining to the specifics of the processing of individuals personal information., i.e. what happens to material that is obtained, what purpose is it being used for, who is operating, who is it shared with and its retention.

Note: processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

3.1.2 All personal data obtained by virtue of the System shall be processed fairly and lawfully and, in particular, shall only be processed in the exercise of achieving the stated objectives of the System When processing personal data, the individual right to privacy in his or her private and family life and home will be respected.

3.1.3 Dover District Council's lawful basis for processing is:

- Law Enforcement Processing (Data Protection Act 2018(DPA18), Part 3) under the Criminal Justice and Public Order Act 1994 s163, Local authority powers to provide closed-circuit television. The council has statutory functions in relation to law enforcement, the prevention, investigation and detection of crime.
- UK GDPR Article 6:
- Processing is necessary for the Council's legitimate interests, in relation to the management of Council land and property, where processing isn't for law enforcement purposes.

3.1.4 Please refer to our Corporate and Community Safety and CCTV Privacy Notice for further information on how we process and protect your personal data and information on the rights under Data Protection Legislation.

3.1.5 Data will be processed securely in accordance with the requirements of the Data Protection Legislation and depending on the Council's purpose for processing, the Law Enforcement Processing (LEP) Regime under Part 3 and/or the UK General Data Protection Regulation (UK GDPR)(Part 2 General Processing) both under the Data Protection Act 2018.

3.2 Data Protection Legislation

3.2.1 For the purposes of The Data Protection Act 2018 the 'data controller' is Dover District Council. We determine the purpose and means of how personal data is processed.

3.2.2 There are two regimes in which Dover District Council's CCTV operate under as detailed in 3.1.3.

3.2.3 The Law Enforcement Processing (LEP) Part 3 of the Data Protection Act 2018

- The majority of the council's personal data processing for CCTV will be handled in accordance with Part 3. This is because the Council is a 'Competent Authority' as defined by the Data Protection Act 2018 Part 3 Section 30(1)(b). Where the council is processing under a law enforcement purpose, the LEP applies.
- The operation of our District CCTV is used for the majority of our cameras for law enforcement purposes, this being the prevention, investigation and detection of crime.

3.2.4 Where processing is for law enforcement purposes, all personal data will be processed in

accordance with the data protection principles set out in Part 3 Sections 35 to 40:

- Processing of personal data for any of the law enforcement purposes is lawful and fair.
- The law enforcement purpose for which personal data is collected is specified, explicit and legitimate as detailed in this code of practice, and;

  Personal data collected is not to be processed in a manner that is incompatible with the purpose for which it was originally collected.

  Personal data collected for any law enforcement purposes may not be processed for a purpose that is not a law enforcement purpose unless the processing is authorised by law.
- Personal data processed for any of the law enforcement purposes is adequate, relevant, and not excessive in relation to the purpose for which it is processed.
- Personal data processed for any of the law enforcement purposes is accurate and, where necessary, kept up to date, and;

  Every reasonable step is taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.
- Personal data processed for any of the law enforcement purposes is kept for no longer than is necessary for the purpose for which it is processed.

  Appropriate time limits have been established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.
- Personal data processed for any of the law enforcement purposes is processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, “appropriate security” includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage)

3.2.5 UK General Data Protection Regulations (UK GDPR)

Personal Data will be processed under the UK GDPR when CCTV is used, and when the purpose isn’t for a law enforcement purpose. This may be to manage property in the ownership and control of the Council (including car parks).

All personal data will be processed in accordance with the principles of GDPR Article 5 and the Council’s Data Protection Policy.

3.3 Access and Exemptions to Information under the Data Protection Act 2018

3.3.1 Any request from an individual for confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data will be directed in the first instance to the Head of Technology & Resilience.

3.3.2 The principles of Sections 45 of the Data Protection Act 2018 and UK General Data Protection Regulations, Article 15 (Rights of Data Subjects and others) shall be followed in respect of every request where processing is undertaken under Part 2 of the Data Protection Act 2018. Those Sections are reproduced at Appendix B.

Any person making a request must be able to prove his identity and provide sufficient information to enable the data to be located. Information appertaining to ‘Subject Access’ is included at Appendix C.

3.3.3 When a request is made for information where processing is carried out solely for law enforcement purposes, individuals are entitled to the following information:

- the purposes for processing and the legal basis we are relying on; categories of personal data you're processing;
- recipients or categories of recipients we are disclosing the personal data to (including recipients or categories of recipients in third countries or international organisations);
- the retention period, or the criteria for determining this; the rights to request rectification, erasure or restriction;
- the ability to raise a complaint with the Information Commissioner and the ICO's contact details; and
- the personal data we are processing (in writing) and any available information you have about the origin of the data.

3.3.4 We can restrict the amount of personal data we supply when it is necessary and proportionate to "protect the rights and freedoms of others." If information contains the personal data of an individual and that of third parties.

3.4 Criminal Procedures and Investigations Act 1996

3.4.1 The Criminal Procedures and Investigations Act 1996 introduced a statutory framework for the disclosure to defendants of material that the prosecution would not intend to use in the presentation of its own case. This material is known as 'unused material'. A summary of the provisions of the Act are contained within the Procedure Manual, but disclosure of unused material under the provisions of this Act should not be confused with the obligations placed on the data controller by Section 45 of the Data Protection Act 2018, known as subject access..

3.5 Criminal Justice and Public Order Act 1994 s163

3.5.1 The Criminal Justice and Public Order Act 1994 s163 provides local authorities with powers to provide closed-circuit television (CCTV) a local authority may take such of the following steps as they consider will, in relation to their area, promote the prevention of crime or the welfare of the victims of crime:

(a) providing apparatus for recording visual images of events occurring on any land in their area;

(b) providing within their area a telecommunications system which, under Part II of the Telecommunications Act 1984, may be run without a licence;

(c) arranging for the provision of any other description of telecommunications system within their area or between any land in their area and any building occupied by a public authority

3.6 Third party requests for information

3.6.1 Data sharing is restricted when the processing is solely carried out under Part 3 of the Data Protection Act 2018. Data sharing can only take place when it is for another law enforcement purpose (whether by the controller that collected the data or by another controller) provided that –

(a) the controller is authorised by law to process the data for the other purpose, and

(b) the processing is necessary and proportionate to that other purpose.

3.6.2 Disclosure for any other purpose would contravene the second data protection principle.

3.6.3 Personal data collected for any of the law enforcement purposes may not be processed for a purpose that is not a law enforcement purpose unless the processing is authorised by law.

3.7 Data Protection Officer

3.7.1 The Owner's Data Protection Officer has responsibilities under the Data Protection Act 2018 and UK General Data Protection Regulation which include monitoring compliance with that legislation and monitoring compliance with the policies of the Council in relation to the protection of this personal data. Notwithstanding any other provision in this Code of Practice, the Council is required by the Data Protection Act 2018 and UK General Data Protection Regulation to provide the Data Protection Officer with access to personal data and processing operations necessary to enable him to discharge any of his legal responsibilities.

Section 4 - Accountability and Public Information

4.1 The Public

4.1.1 Public access to the Control Room will be prohibited except for lawful, proper and sufficient reasons. Visits to the viewing area outside the Control Room will take place from time to time after authorisation by the Head of Technology & Resilience. Visitors will always be accompanied by one of the Designated Officers. Although a visit will only take place in the presence of an authorised operator, he or she will not be expected to take responsibility for such visits but will record the visit as follows:-

- Date, time and duration of visit;
- Authorised person accompanying the visitor or visitors;
- Names and status of visitors; and
- Purpose of visit

All visitors must sign the Visitors' Log, which incorporates a Declaration of Confidentiality.

Any occurrence, which leads to comment during the course of the visit, will also be the subject of record. No visits will take place or continue whilst a live incident is running.

4.1.2 Cameras will not be used to look into private residential property. Where the equipment permits, 'privacy zones' may be programmed into the System. These 'zones' will ensure that the cameras do not survey the interior of any private residence. In addition, all operators will be specifically trained in privacy issues.

4.1.3 A member of the public wishing to register a complaint about any aspect of the System may do so by contacting Dover District Council. All complaints shall be dealt with in accordance with the Council's procedure, a copy of which may be obtained from the offices of Dover District Council or downloaded from the website. Any disciplinary issue identified will be considered under the Council's disciplinary procedures.

4.1.4 All contracted or directly employed CCTV staff are contractually bound by regulations governing confidentiality and discipline.

4.2 System Owner

4.2.1 Designated Officers of the Council, being the nominated representatives of the System Owners, will have unrestricted access to the Control Room.

4.2.2 Head of Technology & Resilience will be responsible for providing regular monthly reports detailing agreed performance indicators to the Director responsible for CCTV, and the relevant Portfolio Holder.

4.2.3 Consultation will normally take place between the owners and the managers of the System with regard to any of its aspects, including this Code of Practice and the Procedure Manual.

4.3 Designated Officers

4.3.1 The Designated Officers will have day-to-day responsibility for the System as a whole. Current Designated Officers are shown at Appendix F.

4.3.2 The relevant Designated Officer will ensure that every complaint is acknowledged in writing within two working days. The Councils target is to provide either a full response or a progress report within ten working days of receiving a complaint. A formal report will be forwarded to the System owner, named at Appendix A, giving details of all complaints and their outcomes.

4.3.3 Statistical and other relevant information, including any complaints made, will be included in the Annual Report of Dover District Council, and will be made available to the public, elected members, the Dover District Community Safety Partnership and other relevant stake holders.

4.4 Public Information

4.4.1 Code of Practice

A copy of this Code shall be published on the Councils' website and will be made available to anyone on request.

4.4.2 Annual Report

A copy of the Annual Report shall be published on the Council's website and will be made available to anyone requesting it.

4.4.3 Signs

Signs will be placed in the locality of the cameras and at main entrance points to the relevant areas, e.g. pedestrian precincts. The signs will indicate:

- The presence of CCTV monitoring;
- The 'owners' of the System;
- The contact telephone number; and
- The purpose of the System.

.

Section 5 - Assessment of the System and Code of Practice

5.1 Evaluation

5.1.1 The System will be evaluated periodically to establish whether the purposes of the System are being met and whether objectives are being achieved. The evaluation will normally include the following:

- An assessment of the incidents monitored by the System;
- A review of the Code of Practice and Procedure Manual;
- A review of the continuing relevancy of the purposes of the System; and Any other factors which have been identified.

5.1.2 The results of any evaluation will be published and will be used to review, develop and make any alterations to the specified purpose and objectives of the scheme as well as the functioning, management and operation of the System.

5.2 Monitoring

5.2.1 The Designated Officers will be responsible for the monitoring, operation and evaluation of the System and the implementation of this Code.

5.2.2 The Designated Officers shall be responsible for maintaining full management and information of incidents dealt with by the Control Room, for use in managing the System and in future evaluations.

5.3 Audit

5.3.1 The District Council's Audit Managers, or nominated deputies, who are not Designated Officers, will be given full access to all systems, when requested subject to satisfactory police vetting.

Section 6 - Human Resources

6.1 Staffing of the control room and those responsible for the operation of the system

6.1.1 The Control Room will be staffed in accordance with the Procedure Manual. Only authorised personnel who have been properly trained to use the System's equipment and in Control Room procedures will operate the System.

6.1.2 Every person involved in the management and operation of the System will be personally issued with a copy of both the Code and the Procedure Manual. He or she will be required to sign to confirm understanding of and adherence to the obligations that these documents place upon him or her and that any breach will be considered a disciplinary offence. He or she will be fully conversant with the contents of both documents, which may be updated from time to time. He or she will comply with both documents as far as is reasonably practicable.

6.1.3 Arrangement may be made for a police liaison officer to be present in the Control Room. Any such person must be conversant with this Code and the associated Procedure Manual.

6.1.4 All persons involved with the System shall receive training in respect of the Code and the Procedure Manual and legislation relevant to their role. Such training will be updated as and when necessary.

6.1.5 The Police must positively vet all persons involved with the System.

6.2 Discipline

6.2.1 Each individual having responsibility under the terms of this Code who has any involvement with the System to which it refers, will be subject to the Authority's Code of Discipline. Any breach of this Code, or of any aspect of confidentiality, will be dealt with in accordance with that Code of Discipline.

6.2.2 The Designated Officers will have primary responsibility for ensuring that there is no breach of security and that this Code is complied with. The Designated Officers will have day-to-day responsibility for the management of the Control Room and for enforcing the Code. Non-compliance with this Code by any person will be considered a severe breach of conduct and will be dealt with accordingly, including, if appropriate, by criminal proceedings.

6.3 Declaration of Confidentiality

6.3.1 Every individual with responsibility under the terms of this Code, who has any involvement with the System to which it refers, will be required to sign a declaration of confidentiality. (See Appendix D. See also Section 8 regarding access to the Control Room by others).

Section 7 - Control and Operation of Cameras

7.1 Guiding Principles

7.1.1 All persons operating the cameras must act with the utmost probity at all times.

7.1.2 Only persons who have been trained in their use and the legislative implications of such use, will operate the cameras and the control, recording and reviewing equipment.

7.1.3 Every use of the cameras will accord with the purposes and key objectives of the System and shall be in compliance with this Code.

7.1.4 Cameras will not be used to look into private residential property. 'Privacy zones' shall be programmed into the System, whenever practically possible, in order to ensure that the interior of any private residential property is not surveyed by the cameras.

7.1.5 System operators will be mindful of exercising prejudices, which may lead to complaints of the System being used for purposes other than those for which it is intended. The operators may be required to justify their interest in, or recording of, any particular individual or group of individuals or property.

7.2 Control

7.2.1 Only staff that are trained and authorised to use the Public Spaces Surveillance system will have access to the operating controls. Those operators will have primacy of control at all times.

7.3 Secondary Control/Monitoring

7.3.1 Secondary monitoring facilities are provided to the Kent Police Control Centre and the KCC Highways Control Centre.

7.3.2 The use of secondary monitoring facilities will be administered and recorded in accordance with this Code and the Procedure Manual. Persons using these facilities must comply with all current legislative requirements.

7.4 Operation of the System by Police

7.4.1 Under some circumstances the Police may make a request to assume direction of the System to which this Code applies. Any requests must be made in writing by a police officer not below the rank of Superintendent. Any such request will only be allowed on the written authority of the Head of Technology & Resilience, or the Director responsible for the CCTV service, or the Chief Executive.

7.4.2 In the event of such a request being allowed, the Control Room will continue to be staffed and operated by those personnel who are authorised to do so and who fall within the terms of Sections 6 and 7 of this Code. They will then operate under the direction of the police officer designated in the written authority.

7.4.3 In extreme circumstances a request may be made by the Police to take total control of the System, including the staffing of the Control Room and control of all associated equipment, to the exclusion of all representatives of the System owners. Any such request must be made to the Designated Officers in the first instance, who will consult personally with the most senior officer of the System owners or designated deputy of equal standing. A request for total exclusive control must be made in writing by a police officer not below the rank of Assistant Chief Constable or person of equal standing.

7.5 Maintenance of the System

7.5.1 To ensure compliance with the Information Commissioner's Code of Practice and to ensure that images recorded continue to be of appropriate evidential quality, the System shall be maintained in accordance with the requirements of the Procedure Manual under a maintenance agreement.

7.5.2 The maintenance agreement will make provision for regular or periodic service checks on the equipment. This will include cleaning of any all-weather domes or housings, checks on the functioning of the equipment, and any minor adjustments that need to be made to the equipment settings to maintain picture quality.

7.5.3 The maintenance will also include regular periodic review and overhaul of all the equipment and replacement of equipment, which is reaching the end of its serviceable life.

7.5.4 The maintenance agreement will also provide for 'emergency' attendance on site by a specialist CCTV engineer to rectify any loss or severe degradation of image or camera control.

7.5.5 The maintenance agreement will define the maximum periods of time permitted for attendance by the engineer and for rectification of the problem, depending upon the severity of the event, and the operational requirements of that element of the System.

7.5.6 It is the responsibility of the Community Safety, Resilience and Digital Manager to ensure appropriate records are maintained in respect of the functioning of the cameras and the response of the contracted maintenance organisation.

Section 8 - Access to, and security of the monitoring room and associated equipment

8.1 Authorised Access

8.1.1 Only trained and authorised personnel will operate the equipment located within the Control Room or equipment associated with the System.

8.2 Public Access

8.2.1 Public access to the monitoring and recording facility will be prohibited except for lawful, proper and sufficient reasons, and only then with the personal authority of the Head of Technology & Resilience. Any such visits will be conducted and recorded in accordance with the Procedure Manual.

8.3 Authorised Visits

8.3.1 Visits by inspectors or auditors do not fall within the scope of the above paragraph and may take place at any time, without prior warning. No more than two inspectors or auditors may visit at any one time. Inspectors or auditors will not influence the operation of any part of the System during their visit. The visit will be suspended in the event of it being operationally inconvenient. Any such visit should be recorded in the same way as that described above.

8.4 Declaration of Confidentiality

8.4.1 Regardless of their status, all visitors to the Control Room, including inspectors and auditors, will be required to sign the visitors' book and a declaration of confidentiality.

8.5 Security

8.5.1 Authorised personnel will normally be always present when the equipment is in use. If the monitoring facility is to be left unattended for any reason it will be secured. In the event of the Control Room having to be evacuated for safety or security reasons, the provisions of the Procedure Manual will be complied with.

8.5.2 The monitoring suite will always be secured by 'Magnetic-Locks' operated by the System operator.

8.5.3 All buildings and rooms storing radio terminals must afford adequate physical protection to the equipment. They should be kept locked when not in use and offer a level of privacy and a degree of resistance to a casual or to deliberate compromise.

8.6 Airwaves Radio

8.6.1 It is essential that minimum-security requirements be adopted in order to protect the confidentiality, integrity and availability of the Airwaves service. Radio terminals must be accounted for at all times, and should be stored securely. Strict radio discipline must be maintained at all times.

8.6.2 Dover District Council uses the current Cabinet Office Code of Practice as a baseline to ensure that minimum standards are maintained. All System Operators are required to read Sections 2 and 3 of the Cabinet Office Code of Practice, which is appended to the procedure manual.

8.6.3 Training will be given to all Operators and there is also a requirement for all Operators to sign a statement to confirm that they understand their responsibilities in relation to the protection of the Airwaves Service. As each System Operator signs on for duty, acceptance of responsibility for the integrity of the Airwaves Service is given. Failure to maintain the required standards may result in disciplinary action being taken.

8.6.4 The Duty Operators Log will be periodically checked at random, and on at least one occasion per month, to ensure that these standards are being maintained.

8.6.5 The System Operator on duty will account for the radio terminal on a daily basis, and this will be audited every 12 months.

8.6.6 Kent Police will monitor voice traffic during all transmissions.

8.6.7 Chief Executive – The ultimate responsibility for the security of the Airwave Service lies with the Chief Executive of Dover District Council. This responsibility cannot be passed to a Managed Terminal Service Provider, or other third party, to own on the Chief Executive's behalf. The

Chief Executive is responsible for clearly defining, documenting and delegating roles and responsibilities for the security of the radio terminals within the organisation.

8.6.8 Radio Terminal Custodian – Head of Technology & Resilience: Delegated by the Chief Executive of Dover District Council, the Radio Terminal Custodian liaises with service providers, radio terminal manufacturers and the accreditation authority (through the Airwave Acrreditation Secretariat) on behalf of the organisation.

The Radio Terminal Custodian is responsible for the following:-

- Ensuring the Airwave Accreditation Secretariat is notified of any changes to the radio Terminal Custodian contact details;
- Ensuring the organisations procedures and documentation reflect the requirements in the latest version of the Cabinet Office Code of Practice;
- Ensuring adequate physical security of all centrally stored Airwave Service radio terminals;
- Maintaining a register to account for the issue and status of all radio terminals and any item of ancillary equipment;
- Conducting an audit of all radio terminals on a regular basis;
- Implementing a continual audit trail for all radio terminals where there may be multiple users (i.e. where pool cars are fitted with mobile radio terminals);
- Ensuring all users are trained in the DDC CCTV Code of Practice;
- Ensuring all authorised radio users sign to accept that they have read and fully understand their responsibilities with regard to this, or the local, Code of Practice;
- If applicable, ensuring divisional or departmental Radio Terminal Custodians are meeting their responsibilities;
- Implementing the appropriate lines of responsibility and conditions of use regarding terminals on loan;
- Implementing robust procedures to ensure a lost, missing or damaged radio terminal is reported and disabled;
- Investigating incidents where tamper seals on radio terminals have been broken; Reporting lost, missing or damaged radio terminals to Kent Police;
- Nominating and training temporary Radio Terminal Custodians, for extraordinary operations (e.g. where terminals are taken abroad);
- Training acting Radio Terminal Custodians (covering annual leave etc) in their duties; and Ensuring secure arrangements are in place for the repair and disposal of radio terminals.

The Radio Terminal Custodian at divisional or departmental level is responsible for a sub-set of the above as delegated.

8.6.9 Line Managers – Head of Technology & Resilience, Community Safety, Resilience and Digital Manager, Community Safety, Resilience & CCTV Team Leader.

The line manager is responsible for the following:-

- Ensuring staff are trained in this Code of Practice;
- Reporting the loss of radio terminals, as directed by the Radio Terminal Custodian in local procedures;
- Reporting damage to radio terminals (including damaged tamper seals), as directed by the Radio Terminal Custodian in local procedures; and
- Ensuring Airwave Service radio terminal use complies with local policies.

8.6.10 Authorised Radio Users – All System Operators

The authorised radio user is directly responsible for the following:-

- Understanding and following the procedures laid out in this Code of Practice; Ensuring the security of any Airwave Service equipment issued to them;
- Reporting the loss of radio terminals, as directed by the Radio Terminal Custodian in local procedures;
- Reporting damage to radio terminals (including damaged tamper seals), as directed by the Radio Terminal Custodian in local procedures; and
- Complying with local policies regarding the use of radio terminals.

Section 9 - Management of Recorded Material

9.1 Guiding Principles

9.1.1 For the purposes of this Code 'recorded material' means any material recorded by, or as the result of, technical equipment, which forms part of the System. This specifically includes images recorded digitally, or by way of video copying, including video prints.

9.1.2 Every video or digital recording obtained using the System has the potential of containing material that has to be admitted in evidence at some point during its life span.

9.1.3 Members of the community must have total confidence that information about their ordinary, everyday activities recorded by virtue of the System, will be treated with due regard to their individual right to respect for their private and family life.

9.1.4 It is of the utmost importance that, irrespective of the means or format of the images obtained from the System, e.g. paper copy, digital media, or any form of electronic processing and storage, they are treated strictly in accordance with this Code and the Procedure Manual. This applies from the moment they are received in the Control Room until their final destruction. Every movement and usage will be meticulously recorded.

9.1.5 Access to recorded material and its use will be strictly for the purposes defined in this Code.

9.1.6 Recorded material will not be copied, sold, otherwise released or used for commercial purposes of any kind or for the provision of entertainment.

9.2 National Standard for the Release of Data to a Third Party

9.2.1 Every request for the release of personal data generated by the System will be channelled through the Head of Technology & Resilience, who will ensure that the principles contained within Appendix C to this Code are followed at all times.

9.2.2 In complying with the national standard for the release of data to third parties, it is intended, as far as is reasonably practicable, to safeguard the rights of the individual to privacy and to give effect to the following principles:

- Recorded material shall be processed lawfully and fairly, and used only for the purposes defined in this Code;
- Access to recorded material will only take place in accordance with the standards outlined in Appendix C and this code; and
- The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

9.2.3 Members of the Police Service or other agencies having a statutory authority to investigate and/or prosecute offences may, subject to compliance with Appendix C, release details of recorded information to the media in an effort to identify alleged offenders or potential witnesses. Under such circumstances, full details will be recorded in accordance with the Procedure Manual.

Note: The Police and Criminal Evidence Act 1984, covers release to the media of recorded information, in any format, which may be part of a current investigation. Any such disclosure should only be made after due consideration of the likely impact on a criminal trial. Full details of any media coverage must be recorded and brought to the attention of both the prosecutor and the defence.

9.2.4 If material is to be shown to witnesses, including police officers, for the purpose of obtaining identification evidence, it must be shown in accordance with Appendix C and the Procedure Manual.

9.2.5 It may be beneficial to make use of 'real-time' video footage for the training and education of those involved in the operation and management of CCTV systems, and for those involved in the investigation, prevention, and detection of crime. Any material recorded by virtue of the System may be used for such bona fide training and education purposes. Recorded material will not be released for commercial or entertainment purposes.

9.3 Recording Policy

9.3.1 Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24-hour period.

9.4 Evidence Provision

9.4.1 In the event of images being required for evidential purposes the procedures outlined in the Procedure Manual will be strictly complied with.

9.5 Digital Recording Devices

9.5.1 The principles established in this section will reflect in the operation of any digital system.

Section 10 – Video Prints

10.1 Guiding Principles

10.1.1 A video print is a copy of an image or images which already exist on a computer disc. Such prints are within the definitions of 'data' and 'recorded material'.

10.1.2 Video prints will not be taken as a matter of routine. When a print is made, it must be capable of justification by the originator, who will be responsible for recording the full circumstances under which the print is taken, in accordance with the Procedure Manual.

10.1.3 Video prints contain data and will therefore only be released under the terms of Appendix C to this Code, 'Release of data to third parties'. If prints are released to the media, in compliance with Appendix C, in an effort to identify alleged offenders or potential witnesses, full details will be recorded in accordance with the Procedure Manual.

10.1.4 A record will be maintained of all video print productions, in accordance with the Procedure Manual. The recorded details will include a sequential number, the date, time and location of the incident, the date and time of the production of the print, the identity of the person requesting the print, (if relevant) and the purpose for which the print was taken.

10.1.5 The records of the video prints taken will be subject to audit in common with all other records in the System.

.

Section 11 - Regulation of Investigatory Powers Act 2000 (RIPA)

Dover District Council have adopted the Home Office document "Covert surveillance and Property interference" and this publication is reproduced at appendix E.

Dover District Council also has a joint working protocol in place with Kent Police, which has been signed by the Chief Executive and a Senior Officer within Kent Police.

Advice and Guidance for Control Room Staff and Police Inspectors in respect of CCTV and the Regulation of Investigatory Powers Act 2000.

The Regulation of Investigatory Powers Act 2000 relates to surveillance by the Police and other agencies and deals in part with the use of directed covert surveillance. Section 26 of this act sets out what is Directed Surveillance. It defines this type of surveillance as:

Subject to subsection (6), surveillance is directed for the purposes of this Part if it **is covert** but **not intrusive** and is undertaken:

(a) for the purposes of a specific investigation or a specific operation;

(b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

(c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance.

CCTV being used intrusively will be authorised other than by this section of the RIP Act. Appropriate guidelines already exist for intrusive surveillance.

The impact for staff in the Police control rooms and CCTV monitoring centres is that there might be cause to monitor for some time a person or premises using the cameras. In most cases, this will fall into sub section (c) above, i.e. it will be an immediate response to events or circumstances. In this case, it would not require authorisation unless it were to continue for some time. The Code says some hours rather than minutes.

In cases where a pre-planned incident or operation wishes to make use of CCTV for such monitoring, an authority will almost certainly be required.

Slow-time requests are authorised by a Police Inspector or above.

If an authority is required immediately, a Police Inspector may do so. The forms in both cases must indicate the reason and should fall within one of the following categories:

An authorisation is necessary on grounds falling within this subsection if it is necessary:-

(a) in the interests of national security

(b) for the purpose of preventing or detecting crime or of preventing disorder

(c) in the interests of the economic well-being of the United Kingdom

(d) in the interests of public safety

(e) for the purpose of protecting public health

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department

or

(g) for any purpose (not falling within paragraph (a) to (f)) which is specified for the purposes of this subsection by an order made by the Secretary of State

Forms will normally originate from the Police, and are entitled “Application for Directed Surveillance Authority Part II RIPA 2000”. This is a restricted document. This document requires the Council’s nominated officer to authorise the operation under the section “seen by a Technical Officer”

No Authorisation Required

When a suspected crime or other incident falling within the objectives of the System is in progress and there is no opportunity to seek prior authorisation.

Appendix A - Key Personnel and Responsibilities

System Owners	System Owner's Data Protection Officer
Dover District Council White Cliffs Business Park Dover Kent CT16 3PJ Tel: 01304 821199	Joe Couchman Data Protection Officer Dover District Council White Cliffs Business Park Dover Kent CT16 3PJ Tel: 01304 872426

System Maintenance Responsibilities

The Head of Technology & Resilience is the single point of reference on behalf of the owners in relation to maintenance issues. The role of the Head of Technology & Resilience and Community Safety, Resilience and Digital Manager, will include a responsibility to:-

i) Ensure the provision and maintenance of all technical equipment forming part of the Dover District Council CCTV System in accordance with contractual arrangements that the owners may from time to time enter into;

ii) Maintain close liaison with the System Operators and the Head of Technology & Resilience;

iii) Maintain liaison with other Designated Officers, with the owners of the System and with operating partners:

iv) Ensure the interests of the owner and other organisations are upheld in accordance with the terms of this Code; and

v) Agree to any proposed alterations and additions to the System, this Code and the Procedure Manual

System Management Responsibilities

The Community Safety, Resilience and Digital Manager will be the single point of reference on behalf of the owner in relation to operational issues. The role will include a responsibility to:-

i) Ensure the operational effectiveness and efficiency of the System in accordance with the terms of the operational contract;

ii) Maintain close liaison with the operational staff;

iii) Maintain liaison with the owner of the System, with other Designated Officers of the System and with operating partners; and

iv) Ensure the interests of the owner and other organisations are upheld in accordance with this Code of Practice

.

Appendix B - Extracts from Data Protection Act 2018 and General Data Protection Regulation

Section 45 The Data Protection Act 2018

1) Subject to the following provisions of this section, an individual is entitled to:

a) Confirmation as to whether or not personal data concerning him or her is being processed and

b) Where that is the case, access to the personal data and the information set out in subsection 2

2) That information is—

(a) the purposes of and legal basis for the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipients to whom the personal data has been disclosed (including recipients or categories of recipients in third countries or international organisations);

(d) the period for which it is envisaged that the personal data will be stored or, where that is not possible, the criteria used to determine that period;

(e) the existence of the data subject's rights to request from the controller -

(i) rectification of personal data (see section 46), and

(ii) erasure of personal data or the restriction of its processing (see section 47);

(f) the existence of the data subject's right to lodge a complaint with the Commissioner and the contact details of the Commissioner;

(g) communication of the personal data undergoing processing and of any available information as to its origin.

3) Where a data subject makes a request under subsection (1), the information to which the data subject is entitled must be provided in writing -

(a) without undue delay, and

(b) in any event, before the end of the applicable time period (as to which see section 54).

4) The controller may restrict, wholly or partly, the rights conferred by subsection (1) to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to

a) avoid obstructing an official or legal inquiry, investigation or procedure;

b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

c) protect public security;

d) protect national security;

e) protect the rights and freedoms of others

(5) Where the rights of a data subject under subsection (1) are restricted, wholly or partly, the controller must inform the data subject in writing without undue delay -

(a) that the rights of the data subject have been restricted,

(b) of the reasons for the restriction,

(c) of the data subject's right to make a request to the Commissioner under section 51,

(d) of the data subject's right to lodge a complaint with the Commissioner, and

(e) of the data subject's right to apply to a court under section 167.

(6) Subsection (5)(a) and (b) do not apply to the extent that the provision of the information would undermine the purpose of the restriction.

(7) The controller must -

(a) record the reasons for a decision to restrict (whether wholly or partly) the rights of a data subject under subsection (1), and

(b) if requested to do so by the Commissioner, make the record available to the Commissioner.

General Data Protection Regulations

1) The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) Where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2) Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Appendix C - National Standard for the Release of Data to Third Parties

Introduction

Public Space Surveillance is arguably one of the most powerful tools to be developed to assist with efforts to combat crime and disorder, whilst enhancing community safety. Equally, it may be regarded by some as the most potent infringement of people's liberty. If users, owners and managers of such systems are to command the respect and support of the general public, Public Space Surveillance Systems must always be used with the utmost probity. They must also use them in a manner, which stands up to scrutiny by the people they are aiming to protect.

Dover District Council believe that everyone has the right to respect for his or her private and family life and home. Although the use of Public Space Surveillance cameras has become widely accepted in the UK as an effective security tool, those people who do express concern tend to do so over the handling of the information (data), which the System gathers.

After considerable research and consultation, the System owners have adopted the nationally recommended standard of The CCTV User Group.

General Policy

All requests for the release of data shall be processed in accordance with the Procedure Manual. All such requests shall be channelled through the data controller.

Primary Request to View Data

Primary requests to view data generated by a CCTV system are likely to be made by third parties for anyone or more of the following purposes:

- Providing evidence in criminal proceedings (e.g. Police and Criminal Evidence Act 1984, Criminal Procedures and Investigations Act 1996, etc);
- Providing evidence in civil proceedings or tribunals; The prevention of crime;
- The investigation and detection of crime (may include identification of offenders and identification of witnesses).

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

- Police;
- Statutory Authorities with powers to prosecute, (e.g. Customs and Excise, Trading Standards, etc);
- Solicitors;
- Plaintiffs and defendants in civil proceedings;
- Accused persons or defendants in criminal proceedings, and;
- Other agencies, (which should be specified in the Code of Practice) according to purpose and legal status.

Upon receipt of a third party of a bona fide request for the release of data, the data controller shall be imposed on such retention, which will be notified at the time of the request.

Where requests are made by plaintiffs, accused persons or defendants the data controller, or nominated representative, shall:

- Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation, and;
- Treat all such enquiries with strict confidentiality

Notes: The release of data to the police is not to be restricted to the civil police but could include, for example, British Transport Police, Ministry of Defence Police, or Military Police. (It may be appropriate to put in place special arrangements in response to local requirements).

Aside from criminal investigations, data may be of evidential value in respect of civil proceedings or tribunals. In such cases, a solicitor, or authorised representative of the tribunal, is required to give

relevant information in writing prior to a search being granted. In the event of a search resulting in a requirement being made for the release of data, such release will only be facilitated on the instructions of a court order or subpoena. A charge may be made for this service to cover costs incurred. In all circumstances data will only be released for lawful and proper purposes.

There may be occasions when an enquiry by a plaintiff, an accused person, a defendant or a defence solicitor, falls outside the terms of disclosure or subject access legislation. An example could be the investigation of an alibi. Such an enquiry may not form part of a prosecution investigation. Defence enquiries could also arise in a case where there appeared to be no recorded evidence in a prosecution investigation.

The data controller shall decide which (if any) 'other agencies' might be permitted access to data. Having identified those 'other agencies', such access to data will only be permitted in compliance with this Standard.

The data controller can refuse an individual request to view if insufficient or inaccurate information is provided. A search request should be reasonably specific, for example, specified to the nearest half-hour.

Secondary Request to View Data

A 'secondary' request for access to data may be defined as, 'any request being made, which does not fall into the category of a primary request'. Before complying with a secondary request, the data controller shall ensure that:

- The request does not contravene, and that compliance with the request would not breach, current relevant legislation, (e.g. GDPR, LEP and The Data Protection Act 2018, Human Rights Act 1998, section 163 Criminal Justice and Public Order Act 1994, etc.);
- Any legislative requirements have been complied with, (e.g. the requirements of GDPR, LEP and The Data Protection Act 2018);
- Due regard has been taken of any known case law (current or past) which may be relevant, (e.g. R v Brentwood BC ex parte Peck: Admn 18 Dec 1997) and;
- The request would pass a test of 'disclosure in the public interest'

If, in compliance with a secondary request to view data, a decision is taken to release material to a third party, the following safeguards shall be put in place before surrendering the material:

- in respect of material to be released under the auspices of 'crime prevention', written agreement to the release of the material should be obtained from a police officer, not below the rank of Inspector. The officer should have personal knowledge of the circumstances of the crime/s to be prevented and an understanding of this Code; and

- if the material is to be released under the heading of 'public well-being, health or safety', written agreement to the release of material should be obtained from a senior officer within the Local Authority. The officer should have personal knowledge of the potential benefit to be derived from releasing the material and an understanding of this Code.

Recorded material may be used for bona fide training purposes such as for police or staff training. Under no circumstances will recorded material be released for commercial sale or entertainment purposes.

Notes: 'Disclosure in the public interest' could include the disclosure of personal data that:

- Provides specific information, which would be of value or interest to the public well-being; Identifies a public health or safety issue; and
- Assists in the prevention of crime.

The disclosure of personal data, which is the subject of a 'live' criminal investigation, would always come under the terms of a primary request.

Individual Subject Access under Data Protection legislation

Under the terms of Data Protection legislation, individual access to personal data, of which that individual is the data subject, must be permitted providing:

- The data controller is supplied with sufficient information to satisfy him as to the identity of the person making the request;
- Sufficient and accurate information is provided about the time, date and place to enable the data controller to locate the information that the person seeks. It is recognised that a person making a request is unlikely to know the precise time. In such circumstances it is suggested that accuracy to within one hour would be a reasonable requirement; and
- In the event of the data controller complying with a request to supply a copy of the data to the subject, only data pertaining to the individual should be copied. All other personal data, which may facilitate the identification of any other person, should be concealed, or erased. Under these circumstances an additional fee may be payable.

The data controller is entitled to refuse an individual request to view data under these provisions if insufficient or inaccurate information is provided. However, every effort should be made to comply with subject access procedures and each request should be considered on its own merits in accordance with data protection legislation.

In addition to the principles contained within the Data Protection legislation, the data controller should be satisfied that the data is:

- Not currently and, so far as can be reasonably ascertained, not likely to become part of a 'live' criminal investigation;
- Not currently and, so far as can be reasonably ascertained, not likely to become relevant to civil proceedings;
- Not the subject of a complaint or dispute, which has not been actioned; The original data and that the audit trail has been maintained;
- Not removed or copied without proper authority.

For individual disclosure only (i.e. to be disclosed to a named subject).

Process of Disclosure

1) Verify the accuracy of the request.

2) Replay the data to the requester only, or responsible person acting on behalf of the person making the request.

3) The viewing should take place in a separate room and not in the control or monitoring area. Only data that is specific to the search request shall be shown.

4) It must not be possible to identify any other individual from the information being shown, (any such information will be blanked-out, either by means of electronic screening or manual editing on the monitor screen).

5) If a copy of the material is requested and there is no on-site means of editing out other personal data, the material shall be sent to an editing house for processing prior to being sent to the requester.

Media Disclosure

Set procedures for release of data to a third party must be followed. If the means of editing out other personal data does not exist on-site, measures should include the following:

In the event of a request from the media for access to recorded material, the procedures outlined under 'secondary request to view data' shall be followed. If material is to be released the following procedures shall be adopted:-

- The release of the material must be accompanied by a signed release document that clearly states what the data will be used for and sets out the limits on its use;
- The release document shall state that the receiver must process the data in a manner prescribed by the data controller, e.g. specific identities or data that must not be revealed;
- The release document shall require that following editing and prior to its use by the media, the data must be passed back to the data controller, either for final approval or consent to its use. This protects the position of the data controller who would be responsible for any infringement of Data Protection legislation and the System's Code; and
- The release document shall be considered a contract and signed by both parties as such. The signatories must have the requisite standing to sign in that capacity on behalf of their respective organisations.

Principles

In adopting this national standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individual's rights to privacy and to give effect to the following principles:

- Recorded material shall be processed lawfully and fairly and used only for the purposes defined in the Code for the CCTV scheme;
- Access to recorded material shall only take place in accordance with this Standard and the Code; and
- The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

Appendix D - Declaration of Confidentiality

The Dover District Council Public Space Surveillance System

I confirm that I am retained as a System Operator.

I have received a copy of the Code of Practice in respect of the operation and management of the Dover District Council Public Space Surveillance System.

I confirm that I am fully conversant with the content of that Code of Practice. I understand that all duties, which I undertake in connection with the Dover District Council Public Space Surveillance System, must not contravene any part of that Code of Practice, or any future amendments to it, of which I am made aware. I undertake that if I am, or become unclear, of any aspect of the operation of the System or the content of the Code of Practice, I will seek clarification from my Manager.

I understand that it is a condition of my employment that I do not disclose or divulge any information, which I have acquired in the course of, or in connection with, my duties to any individual, company, authority, agency or other organisation. This includes information obtained verbally or in writing or by any other media, now or in the future. I understand that this prohibition remains binding after I have ceased to be retained in connection with the Public Space Surveillance System .

In signing this declaration, I agree to abide by, and be bound by, the Code of Practice. I understand and agree to maintain confidentiality in respect of all information gained during the course of my duties, now, or in the future.

I further acknowledge that I have been informed and clearly understand that the communication, either verbally or in writing, to any unauthorised person(s) of any information acquired as a result of my employment with Dover District Council may be an offence against the Official Secrets Act of 1911, Section 2, as amended by the Official Secrets Act of 1989.

.

Signed: ..... Print Name: ..... .

Witness: ..... Position: .....

Dated this ..... (Day) of ..... (Month) .....

Appendix E - Investigatory Powers Act 2016 - Codes of Practice

A copy of this document can be viewed online at:

RIPA Codes of Practice

Or if viewing this document in a paper version:

https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice

Appendix F - Confidential Contact Details

Council Address	Name of Officer	Contact Details
Dover District Council White Cliffs Business Park Dover Kent CT16 3PJ Tel: 01304 821199	Abi Robinson	abi.robinson@dover.gov.uk
	David Parratt	david.parratt@dover.gov.uk
	Elliott Allen	elliott.allen@dover.gov.uk


DOVER
DISTRICT
COUNCIL