DARTFORD
BOROUGH COUNCIL

Dartford CCTV

Code of Practice

Revised May 2019

Index

Page

	Certificate of Agreement	3
Section 1	Introduction & Objectives	4
Section 2	Statement of Purpose and Principles	7
Section 3	Privacy, Disclosure and Data Protection	10
Section 4	Accountability and Public Information	13
Section 5	Assessment of the CCTV System and Code of Practice	15
Section 6	Staffing of Control Room and Discipline	17
Section 7	Control and Operation of Cameras	19
Section 8	Access to, and Security of, Monitoring Room and Associated Equipment	22
Section 9	Management of Recorded Material	26
Section 10	Digital Still Photographs	28
Section 11	Regulation of Investigatory Powers Act 2000 (RIPA)	29
Appendix A	Key Personnel and Responsibilities	30
Appendix B	Disclosure of Data to Third Parties	34
Appendix C	Declaration of Confidentiality – CCTV Operators	40
Appendix D	Declaration of Confidentiality - Lay Visitors	41
Appendix E	Regulation of Investigatory Powers Act Guiding Principles	42
Appendix F	Kent Police & DBC CCTV Joint Working Protocol	44
Appendix G	CCTV Operator's Airwave Radio Declaration	52
Appendix H	Contact Details	53

Certificate of Agreement

The content of this Code of Practice is hereby approved in respect of Dartford Borough Council's Closed Circuit Television 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 Dartford Borough Council

Signature: .....…….....

Name:…Sheri Green……. Position held: Strategic Director (External Services)

Dated the ..... day of 2019

Signed for and on behalf of Kent Police

Signature: .....…….....

Name: ……. Position held: District Commander

Dated the .....…... day of 2019

Section 1 Introduction and Objectives

1.1 Introduction

In summer of 1996, Dartford Borough Council (DBC) introduced a Closed Circuit Television (CCTV) system (hereafter called the CCTV System) which comprises a number of cameras installed at strategic locations within the Borough. Most of the cameras are fully operational with pan, tilt and zoom facilities and a small number are fixed cameras, all with on-site digital recording. There are no recording facilities at any location other than the CCTV Equipment Room situated in the Civic Centre opposite the main CCTV Control Room.

The CCTV System has evolved from the formation of a partnership between Dartford Borough Council and Kent Police (the Partnership), who have both certified their acceptance of the requirements of this Code of Practice (hereafter called the Code).

For the purposes of this document, the 'System Owner' is Dartford Borough Council.

For the purposes of the Data Protection legislation[1] the 'data controller' is Dartford Borough Council.

The system is managed by the System Owner's Community Safety (CCTV) Team. The Designated Officers within this team will be responsible for ensuring CCTV data is processed in accordance with the Data Protection legislation.

The CCTV System has been registered with the Information Commissioner's Office.

Details of the telephone and fax numbers of the System Owner, together with Designated Officer responsibilities are shown at Appendix A to this Code.

1.2 Partnership statement in respect of the Human Rights Act 1998

1.2.1 The Partnership 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 and Data Protection legislation. The Partnership considers that the use of CCTV in the Borough of Dartford is a justified, necessary, proportionate and suitable tool to help reduce crime and the fear of crime and to improve public safety.

[1] Data Protection Act 2018 and General Data Protection Regulation (EU) 2016/679)

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 considered a necessary initiative by the Partnership as it contributes to its duty under the Crime and Disorder Act 1998.

1.2.3 The operation of the CCTV System may be considered an infringement of the privacy of individuals. The Partnership recognises that it is their responsibility to ensure that the CCTV System should always comply with all relevant legislation in order to ensure its legality and legitimacy in a democratic society. The CCTV 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 personal or cultural values, or for the protection of the rights and freedoms of others.

1.2.4 Observance of this Code and the accompanying Protocols and Public Space Surveillance (PSS) Procedure Manual will ensure that evidence is secured, retained and made available as required with due regard to the rights of the individual.

1.2.5 The CCTV System will be operated with respect for all individuals, recognising the individual's right to be free from inhuman or degrading treatment and avoiding any form of discrimination on the basis of (or association to) gender (including transgender), race (including nationality), religion or belief (including non-belief), disability, sexual orientation, age, as well as social background and the other Equality Act 2010 protected characteristics.

1.3 Lawful bases for processing personal data & Objectives of the CCTV System

1.3.1 Most lawful bases require that processing is 'necessary' for a specific purpose. Such **purposes** will include:

- the System Owner's duty to comply with a legal obligation(s) e.g. in the interest of public safety, the prevention and detection of crime, apprehension and prosecution of offenders and for legal proceedings;
- the public task: the processing is necessary for the System Owner to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law;
- in some circumstances - vital interests - where the processing is necessary to protect someone's life

1.3.2 The lawful basis for holding and processing the data will include:

- Section 163 of the Criminal Justice and Public Order Act 1994
- Crime and Disorder Act 1998
- Regulation of Investigatory Powers Act 2000
- Protection of Freedoms Act 2012

See the System Owner's Privacy Notice for Community Safety including CCTV and Environmental Crime

1.3.3 The objectives of the CCTV System, which form the legitimate basis for the processing of data, are:

- To help reduce the fear of crime and anti-social behaviour.
- To help deter crime and assist in the detection of crime and anti-social behaviour.
- In the interests of national security/terrorism.
- To help detect crime and provide evidential material for Police and the Court proceedings for the prosecution of offenders.
- To provide assistance in the overall management of public health and safety within covered areas and improve public protection.
- To enhance community and officer safety and assist in developing the economic well-being of the Dartford Borough.
- To encourage greater use of the Town Centres, shopping areas, car parks and similar locations within the Borough by local residents and visitors, thereby improving the enjoyment of facilities by all that use them.
- To assist the Police and local authority officers in discouraging anti-social behaviour, including alcohol and drug related issues.
- To assist the local councils and statutory partners in their enforcement and regulatory functions within the Borough to make Dartford "the place of quality and choice, a place where people choose to live, work and enjoy their leisure time".
- To assist in traffic management around the Borough of Dartford if and wherever necessary to keep members of the public safe and to ensure the free flow of traffic on local roads that have CCTV coverage.

1.3.2 Within this broad outline, the Dartford Police District Commander, in consultation with the System Owner's Managing Director, may periodically publish and review specific key objectives based on local concerns.

1.4 Protocols & Public Space Surveillance (PSS) Procedure Manual

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

Section 2 Statement of Purpose and Principles

2.1 Purpose

The purpose of this Code is to state the intention of the Partnership to support the objectives of the CCTV System and to outline how it is intended to do so.

2.1.1 The 'purpose' of the CCTV System, and the process adopted in determining the purposes/objectives for implementing it, are as detailed in Section 1 of this Code**.**

2.2 General Principles of Operation

2.2.1 The operation of the CCTV System will recognise the need for formal authorisation of any covert 'directed surveillance' or crime-trend 'hotspot' surveillance, as required by the Regulation of Investigatory Powers Act 2000 and Police related policy.

2.2.2 The CCTV System will be operated with due regard to the relevant definitions, rules and procedures in the Home Office Code of Practice "Covert Surveillance and Property Interference" including the updates published from time to time.

2.2.3 The CCTV System will be operated within the law and in accordance with the JAPAN principles set out in the Human Rights Act. It will only be used for the purposes for which it was established and which are identified in this Code, or which may be subsequently agreed in accordance with this Code.

2.2.4 The CCTV System will be operated with due regard to the principle that everyone has the right to respect for his or her private and family life and home and in accordance with the Data Protection legislation.

2.2.5 The public interest in the operation of the CCTV System will be recognised by ensuring the security and integrity of operational procedures.

2.2.6 Throughout this Code, it is intended, as far as reasonably possible, to balance the objectives of the CCTV System with the need to safeguard the rights of the individual. The System Owner operates a complaints procedure that ensures that is not only accountable, but is seen to be accountable for its CCTV System.

2.2.7 Participation in the CCTV System by any organisation, individual or authority assumes an agreement by all such participants to comply fully with this Code and to be accountable under the Code.

2.3 Copyright & Data Controller

2.3.1 Copyright and ownership of all material recorded by virtue of the CCTV System will remain with the System Owner.

2.3.2 The System Owner is the data controller for the purposes of the Data Protection legislation. Once recorded data has been disclosed to another party, such as the Police, they may then become a 'controller in common' for the processing of that data independently of the System Owner. Both parties should exercise all due diligence in ensuring compliance with the Data Protection legislation.

2.4 Cameras and Area Coverage

2.4.1 This Code refers to those areas within the responsibility of the System Owner. Details of the location of all cameras can be made publicly available.

2.4.2 Transportable or rapidly deployable cameras may be temporarily sited within the Borough. The use of such cameras, and the data produced by virtue of their use, will always accord with the objectives of the CCTV System and is governed by this Code and the PSS Procedure Manual.

2.4.3 Most of the cameras offer full colour, pan tilt and zoom (PTZ) capability, with some automatically switchable to monochrome in low light conditions.

2.4.4 None of the cameras forming part of the CCTV System will be installed in a covert manner. Some cameras may however be enclosed within 'all weather domes', for aesthetic or operational reasons, but the presence of all cameras will be identified by suitable signage.

2.5 PSS CCTV Monitoring and Recording Facilities

2.5.1 A staffed monitoring room, called the Control Room, is located in the Civic Centre Dartford and houses the CCTV equipment, which has the capability of recording all public space surveillance cameras simultaneously throughout every 24-hour period.

2.5.2 Secondary monitoring only equipment may be located in Kent Police premises at their Contact and Control Centre (FCC) with Police Officers now able to view via a Mobile Phone app when on duty.

2.5.3 No equipment, other than that housed within the CCTV Control Room or Equipment Room at the Civic Centre, will be used for recording images from any PSS camera for evidential purposes (but see 2.5.4 below).

2.5.4 CCTV 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 this Code. Only authorised users will operate viewing and recording equipment.

2.6 Human Resources

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

2.6.2 Only CCTV Operators, who are specially selected and trained in accordance with the PSS Procedure Manual, will staff the Control Room.

2.6.3 CCTV Operators should have requisite knowledge and there should be a copy of the legislation for reference including the Human Rights Act 1998, Data Protection legislation, Regulation of Investigatory Powers Act 2000, this Code and the PSS Procedure Manual. Further training will be provided if required.

2.7 Processing and Handling of Recorded Material

2.7.1 All recorded material, whether recorded in analogue or digital format, or as a hard copy Still print, will be processed and handled by a qualified member of staff, strictly in accordance with this Code and the PSS Procedure Manual.

2.8 CCTV 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 this Code and/or the PSS Procedure Manual

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

2.9.2 Minor changes, such as may be required for clarification and which will not have a significant impact, may be agreed by the Strategic Director (External Services), or a nominee identified by him/her.

2.9.3 CCTV Operators may be consulted, opinions sought prior to any changes. Any improvements that the Operators put forward will be considered.

Section 3 Privacy, Disclosure & and Data Protection

3.1 Public Concern

3.1.1 Although members of the public have become accustomed to being observed, when concern is expressed, it is mainly over matters pertaining to the processing of the information, or data, i.e. what happens to material that is obtained?

Note: '***Processing'*** means **obtaining, recording** or **holding** the information or data or **carrying out any operation** or **set of operations** on the information or data, including:

i) Organising, adapting or amending the information or data
ii) Retrieving, consulting about or using the information or data
iii) Disclosing the information or data by transmission, dissemination or otherwise making available, or
iv) Aligning, combining, blocking, erasing or destroying the information or data.

3.1.2 All personal data obtained by virtue of the CCTV System will be processed fairly and lawfully and, in particular, will only be processed in the exercise of achieving the stated objectives of the CCTV System, in accordance with the Data Protection legislation (see section 1.3 of this Code). When processing personal data, the individual's right to privacy in his or her private and family life and home will be respected.

3.1.3 Data will be stored securely in accordance with the requirements of the Data Protection legislation and in accordance with the System Owner's Data Retention and Disposal Policy & Schedule.

3.2 Data Protection legislation

3.2.1 The operation of the CCTV System has been notified to the Office of the Information Commissioner in accordance with the Data Protection legislation.

3.2.2 For the purposes of the Data Protection legislation, the 'data controller' is Dartford Borough Council.

3.2.3 Personal data will be used only for the purposes of, and disclosed only to the persons, including third parties referred to in this Code.

3.2.4 All data will be processed in accordance with the guiding principles of the Data Protection legislation, which include in summary, but are not limited to, the following:

i) All personal data will be obtained and processed fairly and lawfully.
ii) Personal data will be held only for the purposes specified.
iii) Personal data held will be adequate, relevant and not excessive in relation to the purpose for which the data is processed.

iv) Steps will be taken to ensure that personal data is accurate and where necessary, kept up to date.
v) Personal data will be held for no longer than is necessary.
vi) Personal data will be processed in accordance with the rights of the individual data subject.
vii) Appropriate measures will be taken to ensure against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
viii) Personal data will not be transferred to countries outside the European Economic Area unless there is an adequate level of protection for the rights and freedoms of data subjects in place in the intended destination.

3.3 Disclosing personal information - exemptions under the Data Protection legislation

3.3.1 Certain exemptions allow for the disclosure of personal data in situations where there would otherwise be a breach of the Data Protection legislation, or allow information to be withheld from data subjects in circumstances in which it would otherwise need to be disclosed.

The more commonly deployed exemptions are:

1. the disclosure is necessary for the purposes of preventing or detecting crime and the apprehension or prosecution of offenders;
2. the disclosure is necessary for the purposes of maintaining effective immigration control, or the investigation or detection of activities that would undermine the maintenance of effective immigration control;
3. the disclosure is required by an enactment, rule of law or court/tribunal order;
4. the disclosure is necessary for the purposes of actual or prospective legal proceedings, or obtaining of legal advice or establishing, exercising or defending legal rights.

Processing personal data is exempt from the subject access provisions to the extent to which the application of those provisions to the data *would be likely to prejudice* any of the purposes referred to in 1 and 2 above. .

The Council is a signatory to the Kent and Medway information Sharing Agreement. Each application to disclose personal information on the basis of an exemption will be assessed on its own merits. For more information on the application of exemptions, see the System Owner's Guidelines on How to Apply the Data Protection Act 2018 Exemptions

3.4 Criminal Procedures and Investigations Act 1996 (as amended) - The 1996 Act 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 is contained within the PSS Procedure Manual, but disclosure of unused material under the provisions of the 1996 Act should not be confused with the obligations placed on the System Owner to respond to subject access requests pursuant to Section 45 of the Data Protection legislation.

3.5 Subject Access requests

3.5.1 Personal data includes CCTV images of an individual, or images, which give away information about an individual, such as their car number plate.

3.5.2 An individual is only entitled to their own personal data, and not to information relating to other people, (unless the information is also about them or they are acting on behalf of someone). Therefore, it is important that the System Owner establishes whether the information requested falls within the definition of personal data. For further information about the definition of personal data please see the ICO guidance on what is personal data. See also, the System Owner's 'Subject Access Request Guidelines - Dealing with requests from individuals for personal information- How to respond to a SAR' on the intranet.

3.5.3 The Data Protection legislation does not prevent an individual making a subject access request via a third party such as a solicitor. In these cases, the System Owner will need to satisfy itself that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

3.5.4 A child can also request access to information held and shared. Even if a child is too young to understand the implications of subject access rights, it is still the right of the child rather than of anyone else such as a parent or guardian. So, it is the child who has a right of access to the information held about them, even though in the case of young children, these rights are likely to be exercised by those with parental responsibility for them.

3.5.5 Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual (perhaps the perpetrator). The System Owner can refuse to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

(a) the other individual has consented to the disclosure; or
(b) it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information, the System Owner must consider all the relevant circumstances, including:

- the type of information that it would disclose;
- any duty of confidentiality owed to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

This means that although the System Owner may sometimes be able to disclose information relating to a third party, it needs to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the disclosure of information about them, then it would be unreasonable not to do so. However, if there is no such consent, the System Owner must decide whether to disclose the information anyway.

Under the Data Protection legislation, it is an offence to make any amendment with the intention of preventing its disclosure.

3.5.6 Any subject access request from an individual for the disclosure of his/her personal data, which he/she believes is recorded by virtue of the CCTV System, will be directed in the first instance to the Community Safety Manager and dealt with by the CCTV Supervisor, in accordance with the Data Protection legislation.

3.5.7 In supplying the footage, care must be taken not to disclose any personal data of another individual. This may involve 'blurring' parts of the footage such as figures or licence plates.

3.5.8 The information will be provided free of charge. However, a reasonable fee based on the administrative cost of providing the information may be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive. A reasonable fee may also be charged to comply with requests for further copies of the same information.

3.5.9 Any person making a subject access request must be able to prove their identity and provide sufficient information to enable the data to be located.

3.5.10 When responding to a subject access request, the Council cannot apply a policy of blanket non-disclosure. There must be a selected and targeted approach to non-disclosure based on the circumstances of the particular case.

3.5.11 The rights of data subjects are qualified rights and are not absolute. The Data Protection legislation recognises that in some circumstances, the Council might have a legitimate reason for not complying with a subject access request, so it provides a number of exemptions & restrictions from the duty to do so. The most commonly deployed exemptions are:

- where the information is subject to legal or litigation privilege;
- where the information contains the personal data of a third party;
- where the information is of the type, which would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders if disclosed.

3.5.12 Where an exemption or restriction applies to the facts of a particular request, the Council may refuse to provide all or some of the information requested, depending on the circumstances. The application of exemptions/restrictions must be undertaken in consultation with Legal Services.

3.6 Requests by third parties for disclosure of personal data

Third parties may include, but are not limited to:

- Police (civil police, British Transport Police, Ministry of Defence Police, or Military Police)
- Statutory authorities/bodies with powers to prosecute, (e.g. H.M Customs and Excise, Trading Standards etc.)
- Solicitors
- Insurance agencies

Request by third parties are dealt with in accordance with section 9 and Appendix B of this Code.

3.7 Requests by Council employees and members of the public – alleged incidences on System Owner's premises

Requests may be made by the System Owner's employees and members of the public for CCTV footage of activity in/on the System Owner's premises e.g. car parks where criminal damage to vehicles is being alleged.

The ICO advises that consideration should be given to whether the request is genuine and whether there is any risk to the safety of the other people involved.

The Council is in no position to accurately assess the risk posed to individuals when CCTV footage is requested from a private person or group. It will therefore, other only disclose CCTV footage to approved third parties such as Police and Insurance companies. This has no effect on the policy in regards to Data Access Requests

The System Owner will not accept requests from its employees and members of the public for the disclosure (including viewing) of recorded CCTV data.

Vehicle crime should be reported by the individual to Kent Police and/or to their insurance agency.

Section 4 Accountability and Public Information

4.1 The Public

4.1.1 Public access to the Control Room will be prohibited. Visits to the Control Room will take place from time to time after authorisation by the CCTV Management Team. Visitors will always be accompanied by one of the designated officers. Although a visit will only take place in the presence of an authorised CCTV Operator, he or she will not be expected to take responsibility for such a visit but will record the visit as follows:

- Date, time and duration of visit
- Names and status of visitors
- Purpose and/or justification of visit

All visitors will be entered into the Digital Data Log by the CCTV Operator on duty who will inform visitors of the requirement for a Declaration of Confidentiality.

No visits will take place or continue whilst a live incident is running.

4.1.2 Cameras will not be used to look into a private residential property. All residential cameras are fitted with dynamic privacy zones "DPZ". These 'zones' will ensure that the cameras do not survey the interior of any private residence.

4.1.3 A member of the public wishing to register a complaint about any aspect of the CCTV System may do so by contacting a member of the CCTV Management Team (see Appendix H). All complaints will be dealt with in accordance with the System Operator's corporate complaints procedure, a copy of which may be obtained from the offices of System Owner or downloaded from the website www.dartford.gov.uk.

4.1.4 All the System Owner's CCTV staff are contractually bound by regulations governing confidentiality and discipline.

4.2 CCTV Management Team

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

4.2.2 The CCTV Management Team will be responsible for providing regular reports detailing agreed performance indicators to Designated Officers.

4.3 The System Owner's CCTV Team

4.3.1 The Enforcement and Regulatory Services Manager is the head of service with overall management control for the CCTV Team. Day to day management of the CCTV Team is undertaken by the Community Safety Manager. The CCTV Supervisor has day-to-day responsibility for the CCTV System as a whole. The CCTV System is operated by suitably trained and vetted CCTV Operators.

4.3.2 The CCTV System may be subject to an annual audit by an independent local authority - there is currently a rota of place containing a number of member authorities from the Kent CCTV User Group. The CCTV function was last audited in September/October 2017.

4.3.3 The relevant CCTV Team Officer will ensure that every complaint is acknowledged in writing within two working days. Our 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 each of the officer(s), named at Appendix A, giving detail of all complaints and their outcomes.

4.3.4 Statistical and other relevant information, including any complaints made, will be included in the Performance reports of the System Owner. Personal data will be anonymised (see section 4.4.2 of this Code).

4.4 Public Information

4.4.3 Code of Practice

A copy of this Code shall be published on the System Owner's website www.dartford.gov.uk and will be made available to anyone on request. Additional copies will be lodged at public libraries, local police stations and the offices of the System Owner.

4.4.2 Annual Report

The CCTV Team will be responsible for obtaining approval of the Annual Report through its own procedures, prior to making it available to the public. A copy of the Annual Report, when approved, will be made available to anyone requesting it. Additional copies will be lodged at public libraries, local police stations and the System Owner's office.

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. railway and bus stations. The signs will indicate:

- the presence of CCTV monitoring
- the 'owners' of the CCTV System
- the contact telephone number
- the purpose of the CCTV System

Section 5 Assessment of the CCTV System and Code of Practice

5.1 Evaluation

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

- an assessment of the impact upon crime
- an assessment of the incidents monitored by the CCTV System
- an assessment of the impact on town centre business
- an assessment of neighbouring areas without CCTV
- review of this Code of Practice and PSS Procedure Manual
- a review of the continuing relevancy of the purposes of the CCTV System
- an assessment of cost effectiveness, and
- any other factors which have been identified
- assessment of the CCTV Operator's view as to partnership working

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 CCTV System as well as the functioning, management and operation of the CCTV System.

5.2 Monitoring

5.2.1 The CCTV Management Team will be responsible for the monitoring, operation and evaluation of the CCTV System and the implementation of this Code.

5.2.2 The CCTV Management Team will be responsible for maintaining full management information of incidents dealt with by the Control Room, for use in emergency planning scenarios and routine management of the CCTV System. A direct closed internal network link to the equipment is provided in for this purpose.

5.3 Audit

5.3.1 The System Owner's Audit Manager, or nominated deputy, will be given full access to the CCTV System, when requested.

5.4 Lay Visitors

5.4.1 An independent panel of community volunteers, may be appointed to carry out periodic visits to the CCTV Control Room. Accredited lay visitors will be allowed unhindered access to the Control Room at all times unless operational conditions prohibit this.

5.4.2 The purpose of such lay visits is to ensure that, within the constraints of the Data Protection legislation and other relevant legislation, the CCTV System and its management and operation remain as open as possible to public scrutiny.

5.4.3 Lay visitors will be required to be conversant with this Code and the PSS Procedure Manual.

5.4.4 Accredited lay visitors will be asked to monitor CCTV Operators' and managers' adherence to this Code and the PSS Procedure Manual and to report any contravention to the Designated Officers.

5.4.5 Lay visitors will be required to sign a Declaration of Confidentiality and to abide by this Code at all times. (See Appendix D)

5.4.6 Normally, no more than two lay visitors will visit the Control Room at any one time. They will be required to have their personal details entered into the Control Room Digital Data Log and will, as far as practicable, be accompanied by a Designated Officer.

Section 6 Staffing of Control Room & Discipline

6.1 Staffing of the Control Room and those responsible for the operation of the CCTV System

6.1.1 The Control Room will be staffed in accordance with the PSS Procedure Manual. Only authorised personnel who have been properly trained or under training to use the CCTV 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 CCTV System will be personally issued with a copy of both this Code and the PSS 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. He or she should be conversant with the contents of both documents, which may be updated from time to time. He or she will be expected to comply with both documents as far as is reasonably practicable.

6.1.3 Arrangements 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 PSS Procedure Manual.

6.1.4 All persons involved with the CCTV System will receive both BSIA accredited and in post training regarding legislation relevant to their role. Any contracted staff must be SIA licensed.

6.1.5 All persons directly involved with the CCTV System must be vetted by Kent Police, in accordance with Force Policy.

6.2 Discipline

6.2.1 Any breach of this Code, or of any aspect of breach of confidentiality, by Dartford Borough Council employees having responsibility for the CCTV System under the terms of this Code, will be subject to the Council's Disciplinary & Dismissal Policy and Procedure.

6.2.2 The CCTV Management Team 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 for both adhering to and for enforcing this Code. Non-compliance with this Code by any person will be considered as misconduct and will be dealt through the Council's Disciplinary & Dismissal Policy and Procedure.

6.3 Declaration of Confidentiality

6.3.1 Every individual with responsibility under the terms of this Code, who has any involvement with the CCTV System, will be required to sign a separate declaration of confidentiality (See Appendix C). Police officers visiting the Control Room for operational purposes must agree to a declaration of confidentiality by completing and signing the Visitors Log (see section 8 of this Code 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/integrity at all times.

7.1.2 Only persons, who are trained in or training 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 CCTV System and in compliance with this Code.

7.1.4 Both permanent and movable cameras must be sited and image capture restricted to ensure that they do not view areas that are not of interest and are not intended to be the subject of surveillance, such as individuals' private property. 'Privacy zones' will be programmed into the CCTV System, whenever practically possible, in order to ensure that the private residential property is not surveyed by the cameras.

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

7.2 CCTV Control Room

7.2.1 Only staff who are trained or being trained and authorised to use the CCTV equipment will have access to the operating controls including the maintenance contractors and CCTV Management Team who will also have primacy of control at all times.

7.2.2 Control Room Digital Data Log

The Digital Data Log will be owned and maintained by the CCTV Manager. This will be used daily by trained staff in the Control Room from a Council based computer. The on- duty CCTV Operator will record all events occurring during the hours of operation. This will also act as an evidential log for audit proposes with Kent Police and other outside agencies. This Digital Data Log will be used and have all day to day operations in the Control Room entered, from Police footage requests to shift changeovers, calls made in respect of the CCTV System from Kent Police and other agencies, visitors to the Control Room, and observations around the Town Centre. CCTV System performance and faults on the CCTV System will also be reported in the Digital Data Log. This Digital Data Log is also used to generate a weekend report that is sent to some members of the Community Safety Unit (CSU). This is a restricted document and will only be passed on to members of the CSU and members of the Community Safety Partnership in accordance with the Kent and Medway Information Sharing Agreement.

7.3 Secondary (viewing) Monitoring

7.3.1 Secondary (viewing only) monitoring facilities are provided at Kent Police Force Contact and Control Centre at Maidstone (FCC) where they have the ability to forward live images onto a secure Police Mobile Phone App when on duty. There is also an additional monitoring facility established at a secure location for the purposes of “out of hours” administration and maintenance of the CCTV System by a member of the CCTV Management Team.

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

7.3.3 If available and subject to permission being granted by a CCTV Management Team member, or a senior CCTV Operator, secondary control rooms may take control of the operation of the cameras. The use of secondary control and monitoring facilities will be administered and recorded in full accordance with this Code and the PSS Procedure Manual. Persons using these facilities must comply with all current legislative requirements.

Note: There are currently no facilities (DRC) in place to carry out any kind of secondary control of CCTV Camera PTZ movements.

7.4 Operation of the CCTV System by the Police

7.4.1 Under some circumstances, the Police may make a request to assume direction of the CCTV System. 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 Strategic Director, External Services of the System Owner, or designated deputy of equal standing.

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 8 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 CCTV System, including the staffing of the Control Room and control of all associated equipment. Any such request must be made to the CCTV Management Team in the first instance, who will consult personally with the Strategic Director of External Services of the System Owner 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 Superintendent or nominated officer. A member of the CCTV team will be present at all time during this takeover of the facility.

7.5 Maintenance of the CCTV System

7.5.1 To ensure compliance with the Information Commissioner's 'Practice for surveillance cameras' and to ensure that images recorded continue to be of appropriate evidential quality, the CCTV System will be maintained in accordance with the requirements of the PSS Procedural 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 CCTV System.

7.5.6 It is the responsibility of the CCTV Management Team 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 the Security of, CCTV Control Room and Associated Equipment

8.1 Authorised Access

8.1.1 Only authorised personnel will operate the equipment located within the Control Room or equipment associated with the CCTV 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 authority of the CCTV Management Team. Any such visits will be conducted and recorded in accordance with the PSS Procedure Manual.

8.3 Authorised Visits

8.3.1 Visits by lay visitors 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 CCTV 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 have personal details entered into the Digital Data Log and read declaration of confidentiality.

8.5 Security

8.5.1 Authorised personnel will normally be present at all times when the equipment is in use. If the monitoring facility is to be left unattended for any reason CTV Operators should be logged out. In the event of the Control Room having to be evacuated for safety or security reasons, the provisions of the PSS Procedure Manual will be complied with.

8.5.2 The Control Room will at all times be secured by ‘Magnetic-Locks’ operated by the CCTV Operator, ‘Digi-Locks’ requiring an alpha numeric code for entrance, or other equally secure means.

8.6 Airwaves Radio

It is essential that appropriate security requirements are 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.

The System Operator applies the current Cabinet Office Code of Practice as a baseline to ensure that minimum standards are maintained. All CCTV Operators are required to read Sections 2 and 3 of the Cabinet Office Code of Practice, which is appended to the PSS Procedure Manual.

Training will be given to all CCTV Operators and there is also a requirement for all CCTV Operators to sign a statement to confirm that they understand their responsibilities in relation to the protection of the Airwaves Service. As each CCTV 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.

The Duty CCTV Operator's Digital Data Log will be periodically checked daily by the CCTV Supervisor at random, and on at least one occasion per week, to ensure that these standards are being maintained.

The radio terminal will be accounted for on a daily basis by the CCTV Operator on duty, and this will be audited every 12 months.

Kent Police may monitor voice traffic during all transmissions.

8.7 Roles and Responsibilities

8.7.1 The Council's Managing Director

The ultimate responsibility for the security of the Airwaves Service lies with System Owner's Managing Director. This responsibility can be delegated by the Managing Director, to a Managed Terminal Service Provider, or other third party.

The Managing Director is responsible for clearly defining, documenting and delegating the roles and responsibilities for the security of the radio terminals within the System Owner's organisation.

8.7.2 Radio Terminal Custodian - CCTV Supervisor

The Radio Terminal Custodian liaises with service providers, radio terminal manufacturers, ***CINRAS***[2] (Comsec Incident Notification, Reporting and Alerting System) and the accreditation authority (through the Airwave Accreditation Secretariat), on behalf of the System Owner.

The Radio Terminal Custodian is responsible for the following:

[2] **C**omsec **I**ncident **N**otification, **R**eporting and **A**lerting **S**ystem (**CINRAS**) is managed, on a 24 hour basis, by CESG.

- 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 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 CINRAS;
- 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.

8.7.3 Supervisors/Line Managers

The CCTV Supervisor s 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 Airwaves Service radio terminal use complies with local policies.

8.7.4 Authorised Radio Users – CCTV Operators

The authorised radio user, by signing the Airwave Declaration in Appendix G, agrees to be 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 CCTV System. This specifically includes images recorded digitally, or by way of data copying, including still prints.

9.1.2 Every digital recording obtained using the CCTV System has the potential of containing material that has to be admitted in evidence at some point during its life span and will all be individually numbered.

9.1.3 Members of the community must have total confidence that information about their ordinary, everyday activities recorded by virtue of the CCTV 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 media or format of the images obtained from the CCTV System, e.g. Paper Copy, Hard Disc Drive, DVD, CD, or any form of electronic processing and storage, they are treated strictly in accordance with this Code and the PSS Procedure Manual. This applies from the moment they are received in the Control Room until their final 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 other than 3rd parties/Insurance requests.

9.2 Disclosure of Data to a Third Party

9.2.1 Every request for the release of personal data generated by the CCTV System will be channelled through the CCTV management Team. The Designated Officers will ensure that the principles in Appendix B to this Code are followed at all times.

The disclosure of personal data for commercial or entertainment purposes is specifically prohibited.

9.2.2 The Police or other agency having a statutory authority to investigate and/or prosecute offences may, subject to compliance with Appendix B, 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 PSS 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 disclosed to witnesses, including Police officers, for the purpose of obtaining identification evidence, it must be disclosed in accordance with Appendix B and the PSS 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 the CCTV System, and for those involved in the investigation, prevention and detection of crime. Any material recorded by virtue of the CCTV 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 Digital system – Provision & Quality

9.3.1 To ensure the quality of footage, and that recorded information meets the criteria outlined by current Home Office guidelines, only WORM (Write Once Read Many) media of good quality are used on the CCTV System.

9.4 Information – Retention

9.4.1 Recorded media will be retained for a maximum period of 6 months to establish if "non-evidential" or similar. Before deletion or destruction, each disc will be erased, in accordance with the manufacturer's requirements and full details will logged on the Digital Data Log and destroyed evidence logged.

9.5 Recording Policy

9.5.1 Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24-hour period for a period of 31 days after which the data is automatically overwritten.

9.5.2 Images from selected cameras will be recorded in real time (25 images per second) at the discretion of the CCTV Operators or as directed by Designated Officers.

9.6 Evidential Material

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

Section 10 Digital Still Photographs

10.1 Guiding Principles

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

10.1.2 Digital still photographs will not be taken as a matter of routine. When a still image is recorded, it must be capable of justification by the originator, who will be responsible for recording the full circumstances under which the still is taken, in accordance with the PSS Procedure Manual an individually numbered.

10.1.3 Digital still photographs contain personal data and will therefore only be disclosed under the terms of Appendix B to this Code, 'Disclosure of data to third parties'. If stills are released to the media, in compliance with Appendix B, in an effort to identify alleged offenders or potential witnesses, full details will be recorded in accordance with the PSS Procedure Manual.

10.1.4 A record will be maintained of all digital still photograph productions, in accordance with the PSS 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 digital still photographs taken will be subject to audit in common with all other records in the CCTV System.

Section 11 Regulation of Investigatory Powers Act 2000 (RIPA)

11.1 Guiding Principles

11.1.1 The System Owner has adopted a Policy Statement in relation to the Regulation of Investigatory Powers Act 2000. This Policy Statement complies with Home Office guidance and is periodically audited by IPCO (Investigatory Powers Commissioner). An annual report on the use of RIPA is submitted by the System Owner, to IPCO.

11.1.2 The System Owner has a joint working protocol in place with Kent Police with regard to the use of Public Space CCTV Systems for surveillance authorised by the Regulation of Investigatory Powers Act 2000. This protocol has been signed by the Council's Managing Director and a senior ranking officer within Kent Police and is reproduced in Appendix F.

11.1.3 Advice and guidance for CCTV Control Room staff and Police officers in respect of PSS CCTV Systems and the Regulation of Investigatory Powers Act of 2000 is reproduced in Appendix F.

Appendix A

Key Personnel and Responsibilities

1. System Owner — **Dartford Borough Council**

The system is managed by the Head of Enforcement and Regulatory Services (EARs)

Address	**Civic Centre** **Home Gardens** **Dartford** **Kent DA1 1DR**
Telephone Number	**01322 343434**
Fax Number	**01322 343607**

2. CCTV Management Team Responsibilities

Designated Officer(s) from Dartford Borough Council will be the single point of reference in relation to operational issues. The role will include a responsibility to:

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

ii) Agree to any proposed alterations and additions to the CCTV System, this Code of Practice and the PSS Procedure Manual

3. CCTV System Maintenance Responsibilities

Designated Officer(s) from Dartford Borough Council will be the single point of reference in relation to maintenance issues. The role will include a responsibility to:

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

ii) Agree to any proposed alterations and additions to the CCTV System, this Code and the PSS Procedure Manual.

Appendix B

Disclosure of Data to Third Parties

1. Introduction

CCTV is arguably one of the most powerful tools to be developed during recent years 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, CCTV systems must be used with the utmost probity at all times and in a manner which stands up to scrutiny by the people they are aiming to protect.

Everyone has the right to respect for his or her private and family life and home. Release of data to third parties must comply with the principles outlined in the Kent and Medway Information Sharing Agreement and guidance issued from time to time, by the Information Commissioner and other relevant bodies such as the Home Office.

2. General Policy on disclosure/sharing

Many of the lawful bases for disclosing/sharing information depend on the processing being 'necessary' for a specified purpose (see section 1.3 of this Code). Disclosure/sharing of information must be a targeted and proportionate way of achieving the purpose.

On a request for disclosure/sharing, the System Owner must satisfy itself that the requester has cited a specified, explicit and legitimate purpose for the disclosure/sharing of data to it by the System Owner. This means that the reason(s) for each instance of a disclosure (including viewing)/sharing of data must be set out clearly by the requester, including their reliance on any Data Protection legislation exemptions and justification for reliance on the exemptions – see the Kent and Medway Information Sharing Agreement.

All requests for the release of data will be processed in accordance with the PSS Procedure Manual.

3. Requests to view/disclose data

a) Requests are likely to be made by third parties for any one or more of the following:

i. to aid with the detection or prevention of crime;
ii. for reasons related to the detection and prevention of terrorism;
iii. to aid with the detection and prevention of non-criminal acts that are nevertheless unlawful;
iv. to address anti-social behaviour;

v. for the purposes of actual or prospective legal proceedings, or obtaining of legal advice or establishing, exercising or defending legal rights.

See also section 1.3 of this Code.

3. Media disclosure

The Data Protection legislation exemption (Schedule 2, part 5, para 26(3) of the Data protection Act 2018[3]) applies to journalism but this should not be construed as an automatic blanket exemption from the Data Protection legislation - the media must still ensure they give consideration to the data protection rights of individuals.

The System Owner must be satisfied that the disclosure is lawful, sufficiently justified in the public interest and would be fair and meet the 'legitimate interests' condition[4]. If the information in question is sensitive personal data (someone's health, sex life or allegations of criminal activity), there is a specific Data Protection legislation condition to allow a public interest disclosure to journalists if it is related to wrongdoing or incompetence, but otherwise, the System Owner will need to be satisfied that one of the conditions for processing sensitive data applies (see the Kent and Medway Information Sharing Agreement). The key is proportionality. It is a balancing act – if there is a serious privacy intrusion or risk of harm, the media will need to demonstrate/establish a significant public interest to justify the disclosure.

The Data Protection legislation does not oblige the System Owner to disclose information to the media, if it disagrees with the media's view of the public interest, or if the System Owner has other overriding legal, professional or reputational reasons to refuse to disclose the information.

Before disclosing information to the media, the System Owner must ensure that the request cites an appropriate public interest justification.

4. Disclosure to insurance agencies

The disclosure of recorded data will be on the authority of the CCTV Supervisor and dealt with in accordance with the PSS Procedure Manual.

A request can be made through the relevant online form on the System Owner's website www.dartford.gov.uk. The request will be dealt with once payment for disbursements (a minimum fee of £55) is received by the System Owner. All information regarding the footage will be logged in the Control Room Digital Data log.

[3] Stipulates that the disapplication of certain GDPR provisions for journalists will apply 'to the processing of personal data carried out for the special purposes, whether or not the data are being processed for a second or ancillary purpose'

[4] Legitimate interests will include a media organisation's commercial and journalistic interests in gathering and publishing material, as well as the public interest in freedom of expression and the right to know

5. Disclosure to the Police

The disclosure of recorded data will be on the authority of the CCTV Supervisor and dealt with in accordance with the PSS Procedure Manual.

Disclosure will be in accordance with the Kent and Medway information Agreement, including the submission of Form 3560 v1 , by the Police which will cite a specified, explicit and legitimate purpose for the disclosure/sharing of data to it by the System Owner. This means that the reason(s) for each instance of a disclosure (including viewing)/sharing of data must be set out clearly by the Police, including their reliance on any Data Protection legislation exemptions and justification for reliance on the exemptions.

Appendix C

Declaration of Confidentiality – CCTV System Operators

The Dartford Borough Council CCTV System

I confirm that I am employed as a CCTV Operator.

I have received a copy of the Code of Practice in respect of the operation and management of the Dartford Borough Council's CCTV System.

I confirm that I am conversant with the content of that Code of Practice. I understand that all duties, which I undertake in connection with the Dartford Borough Council's CCTV 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 CCTV 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 the media. This includes information obtained verbally or in writing or by any other means, now or in the future. I understand that this prohibition remains binding after I have ceased to be retained in connection with the CCTV 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.

Signed: …..... Print Name: .....……

Witness: ……..... Position: .....……

Dated this ……. (Day) of ….....…. (Month). 20…….

Appendix D

Declaration of Confidentiality - Lay Visitors

I am a Lay Visitor of the Dartford Borough Council's CCTV System with a responsibility to monitor the operation of the System and adherence to the Code of Practice. I have received a copy of the Code in respect of the operation and management of that CCTV System.

I confirm that I am fully conversant with my voluntary duties and the content of the Code of Practice. I undertake to inform the Designated Officers of any apparent contravention of the Code of Practice that I may note during the course of my visits to the monitoring facility.

If now, or in the future I am, or I become unclear of any aspect of the operation of the CCTV System or the content of the Code of Practice, I undertake to seek clarification of such uncertainties.

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

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 voluntary duties, now, or in the future.

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

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

Dated the .....…… (Day) of…….(Month) 20……..

Appendix E

Regulation of Investigatory Powers Act Guiding Principles

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 Superintendent or above.

If an authorisation 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

In cases where there is doubt as to whether an authorisation is required or not, it may be prudent to obtain the necessary authority verbally, followed by written confirmation using the forms. Any authority given should be recorded appropriately for later reference. This should include the name of the officer authorising.

Forms should be available at each CCTV monitoring centre and are included in the PSS Procedure Manual and available from the CCTV User Group Website.

Examples:

Inspector's Authorisation
An example of a request requiring an Inspector's authorisation might be where a car is found in a car park late at night and is known to belong to drug dealers. The officers might task CCTV to watch the vehicle over a period of time to note who goes to and from the vehicle.

Superintendent's Authorisation
An example here might be where it is suspected that shop premises are being utilised for dealing in stolen goods and crime squad officers wish to use CCTV to monitor the premises from the outside for a period of days.

No Authorisation Required
An example might be where officers chance upon local drug dealers sitting in the town centre and, in order not to divulge that observation is taking place, ask for CCTV to monitor them.

Appendix F

Kent Police & DBC CCTV Joint Working Protocol

Kent Police

Public Space CCTV Systems

A protocol for their use for surveillance, authorised by the Regulation of Investigatory Powers Act 2000 between the Local Authorities in Kent and Medway and Kent Police.

February 2018

CONTENTS

1. **Introduction**
2. **Directed Surveillance**
3. **Intrusive Surveillance**
4. **Authorisation Procedure**
5. **Conduct of Surveillance**
6. **Product of Surveillance**
7. **Sensitive Cases**
8. **Disclosure**
9. **Conduct within CCTV suites**
10. **Complaints**

1. Introduction

1.1. This Protocol between the local authorities within Kent and Medway, and the Kent Police is to cater for the use of public space CCTV systems operated by the local authorities in police operations in circumstances that may require authorisation under the Regulation of Investigatory Powers Act 2000 (RIPA).

1.2. The Office of Surveillance Commissioners (OSC) Procedures and Guidance (December 2008) states: *"It is recommended that a law enforcement agency should obtain a written protocol with a local authority if the latter's CCTV system is to be used for Directed Surveillance. Any such protocol should be drawn up centrally in order to ensure a unified approach. The protocol should include a requirement that the local authority should see the authorisation (redacted if necessary to prevent the disclosure of sensitive information) and only allow its equipment to be used in accordance with it."*

1.3. CCTV schemes operated by local authorities are intended primarily to carry out overt surveillance for the safety and reassurance of the public. The overt operation of CCTV schemes and co-operation between the local authorities and Kent Police in response to incidents does not require authorisation under RIPA and is not subject to this Protocol. The overt use of CCTV is governed by the Data Protection legislation and the CCTV Code of Practice published by the Information Commissioner's Office.

1.4. RIPA is permissive legislation that allows law enforcement agencies and public authorities to carry out surveillance. The Act defines two categories of surveillance activity, directed surveillance and intrusive surveillance.

1.5. As public authorities specified by the act, police forces and local authorities are able to carry out surveillance authorised under RIPA. Where two public authorities are working together an authorisation obtained by one authority can cover the activities of the other. Therefore it is not necessary for local authorities to obtain their own authorisation when they are acting in support of the police.

1.6. However, advice from the Office of Surveillance Commissioners states that: *"Local authorities have a keen interest in ensuring that authorisations are properly implemented even when acting on behalf of others, such as the police, since the product is primarily theirs and it may be they who receive the complaints or claims in the case of misuse."*

1.7. To enable the relevant local authority to fulfil this duty Kent Police will provide the local authority with sufficient information to demonstrate that proper authorisation is in place.

2. Directed Surveillance

2.1. Directed Surveillance is surveillance that 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.

2.2. The day-to-day use of public space CCTV systems does not normally require authorisation under RIPA. This is because the cameras are not covert and the targeting of any individual person for surveillance is by way of immediate response to events.

2.3. However, where CCTV cameras are used as part of a planned covert operation, to carry out surveillance of an identified individual or a location, in a way that is likely to obtain private information about any person, then an authorisation for directed surveillance is likely to be required.

2.4. Where Kent Police is planning to carry out surveillance with the co-operation of the local authority using a CCTV system, Kent Police will obtain the authorisation.

3. Intrusive Surveillance

3.1. It is highly unlikely that Kent Police will ever seek assistance from a local authority to carry out intrusive surveillance using a public CCTV system. The main purpose of including the information in this section is to make clear the limitations of what can be done under an authorisation for directed surveillance.

3.2. Intrusive Surveillance is surveillance that:

a. Is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

b. Involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

3.3. For the purposes of this part of RIPA surveillance which:

a. Is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle, but

b. Is carried out without the device being present on the premises or in the vehicle,

Is not intrusive unless the device is such that it **consistently** provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

3.4. It should be noted that a view into residential premises or a private vehicle is not necessarily intrusive surveillance as defined in RIPA. **For example a chance view through a window would not render surveillance intrusive, the issue for consideration is whether information of the same quality and detail as from a device inside the premises would be obtained.** However, if the sole purpose of the surveillance is to look into residential premises this is likely to be intrusive.

3.5. Local authorities are not empowered to authorise intrusive surveillance, but they may provide operational support to a police operation, where the authorisation allows this. Therefore if the need for such support is foreseen, it should be specified in the authorisation. However as stated in paragraph 3.1, it is highly unlikely that such a request would ever be made.

4. Authorisation Procedure

4.1. There will be two distinct circumstances where police will make an approach to a local authority to request the use of their CCTV facility for directed surveillance.

a. A **pre-planned operation** with a Superintendent's written authority.

b. An **unplanned urgent operation** with a Superintendent's verbal authority or an Inspector's written authority.

4.2. In a **pre-planned operation** it is recommended that prior to making an application for directed surveillance involving the use of a CCTV system, the police applicant should make contact with the CCTV manager to discuss the feasibility of the proposed surveillance and to reach agreement in principle as to what can be achieved. This discussion and the subsequent application should include:

- Why directed surveillance is required.
- What CCTV will capture.
- What the role of the CCTV Operator will be.
- When the surveillance is anticipated to start and end.

4.3. The wording on the police application and authorisation form must encompass the use of the CCTV system e.g. "Static surveillance and the technical means necessary to monitor and record such surveillance".

4.4. Before the surveillance commences the police applicant will provide the CCTV Manager with a copy of the signed authority, redacted if necessary to protect sensitive operational information.

4.5. In an **unplanned urgent operation**, the police applicant will provide the CCTV Manager with the following information:

a. The names of the applicant and authorising officer

b. The date and time of the authorisation and expiry (72hrs).

c. Details of the nature of the surveillance authorised that relates to the CCTV scheme.

d. Details of the persons (known or unknown) who are subject of the surveillance.

e. A copy of the signed authority will be provided within 3 working days.

4.6. In both planned and unplanned urgent operations, the police applicant will subsequently provide the CCTV Manager with:

a. Details of any changes (e.g. addition or removal of subjects), resulting from any REVIEW of the authority.

b. A copy of any RENEWAL of the authority (redacted if necessary).

c. A copy of the CANCELLATION of the authority (redacted if necessary).

5. Conduct of Surveillance

5.1. Care must be taken to ensure that where surveillance is authorised under RIPA the surveillance subsequently carried out does not exceed what is authorised.

5.2. The police officers and local authority staff involved in carrying out surveillance under this protocol must be fully briefed about the extent of the surveillance authorised and that it must not be exceeded.

5.3. If during the course of the surveillance it becomes apparent that the circumstances have changed to the extent that the original authorisation is no longer sufficient, the police officer in charge of the surveillance and the senior CCTV Operator present should consider whether the change in circumstances is part of the original operation. If it is not, they should consider whether surveillance could continue without authorisation as an immediate response to events, see paragraph 2.1(c) above. If continued surveillance is not in immediate response to events a further authority should be obtained, verbally if appropriate.

6. Product of Surveillance

6.1. In most circumstances the product of the surveillance will be visual images captured on videotape or as digitally recorded files. Police officers may also keep a written surveillance log.

6.2. The requirement to retain the product will vary depending on the nature of the surveillance. In the case of the surveillance of an individual suspected of involvement in crime it is likely that all images of the individual and associates will need to be retained.

6.3. The police officers carrying out the surveillance will specify the material that is required as evidence or as part of surveillance records.

6.4. The local authority staff will supply recordings of the material requested in a format that can be viewed by the police and at court.

6.5. Evidence obtained during planned surveillance should be treated in the same manner as evidence obtained during the normal operation of the scheme. The Code of Practice that accompanies the Criminal Procedure and Investigations Act 1996 contains guidance on the period that evidence should be retained.

6.6. In the case of material retained as evidence of a crime, or as part of surveillance records, the investigating officer will be responsible for arranging the destruction of the material when it is no longer required.

7. Sensitive Cases

7.1. In cases that require a high level of secrecy Kent Police should make contact with a designated senior manager within the local authority to discuss any special arrangements that may be required.

8. Disclosure

8.1. The Data Protection legislation provides numerous exemptions in respect of personal data (see section 3.4 above).

8.2. The Freedom of Information Act 2000 gives a general right of access to all types of recorded information held by public authorities. The Act sets out exemptions from that right.

8.3. In the event of requests under the Data Protection Act or the Freedom of Information Act for access to data held by the local authority in respect of surveillance carried out jointly with Kent Police, the local authority should seek guidance from Kent Police as to whether disclosure would prejudice the investigation of crime.

8.4. It is important that any response to such enquiries does not disclose by inference whether or not surveillance has taken place. It may seem harmless where surveillance has not taken place to respond to that effect, however by doing this any other response on another occasion would indicate that it had taken place.

9. Conduct within CCTV suites

9.1. Police officers attending CCTV suites within police, local authority or other premises will identify themselves fully and show their warrant cards when in plain clothes.

9.2. Police officers will book in and out of the suite and comply with the local procedures within the particular suite as directed by the CCTV staff in attendance.

10. Complaints

10.1. Complaints received by Kent Police concerning the 'Direction and Control of the force' over the use of surveillance, which has included the use of a local authority CCTV system, will be dealt with in accordance with Kent Police policies and procedures.

10.2. Complaints that relate specifically to the conduct of a police officer or a member of police staff are complaints subject to the Police Reform Act 2002 and will be dealt with by the Professional Standards Department.

10.3. Complaints under section 65, Regulation of Investigatory Powers Act 2000, concerning surveillance that has taken place in 'challengeable circumstances' will be referred to the Investigative Powers Tribunal.

10.4. Kent Police will inform the local authority whenever any complaint is received relating to the use of surveillance, which has included the use of a local authority CCTV system, and of the outcome of any investigation, but not including complaints of conduct matters falling within the Police Reform Act.

10.5. In the event of any complaint being received by the local authority about surveillance that has been initiated by Kent Police, The Authority should refer to Kent Police Professional Standards Department to discuss the investigation of the complaint.

10.6. Local authorities may carry out their own investigations, in doing so they should have regard for the potential compromise of criminal investigations and whether any matters are sub udice.

Signed: **.....**

For and on behalf of

Dartford Borough Council

Name:

Position:

Date:

Signed: **……**

For and on behalf of

Kent Police

Name:

Position:

Date:

Appendix G

CCTV Operator's Airwave Radio Declaration

DARTFORD BOROUGH COUNCIL

I confirm that I am employed as a CCTV Operator for Dartford Borough Council.

I have read a copy of the Cabinet Office Code of Practice Issue v3.0 November 2007 in respect of the Secure Handling and Use of Airwave Service Radio Terminals and that I understand my responsibilities that are contained therein.

Signed: …..... Print Name: .....……

Witness: ……..... Position: .....……

Dated this ……. (Day) of ….....…. (Month). 20…….

Appendix H

CONTACT DETAILS - CONFIDENTIAL

CCTV Management Team Officer	Job Description	Contact Details
Main DBC Switchboard		Telephone: 01322 343434
Mr M Salisbury(ddl)	***Head of Service, Enforcement and Regulatory Services***	Telephone: 01322 343339
Mr A Henley (ddl)	***Community Safety Manager***	Telephone: 01322 343502
Mr K Castle(ddl)	***CCTV Supervisor***	Telephone: 01322 343383