Code of Practice

for the operation of the

Public Space

Closed Circuit Television

in

Bournemouth Poole & Christchurch

April 2019

Contents

Contents **Page**

1. Introduction

1.1 Why use Closed Circuit Television?

The use of closed-circuit television (CCTV) technology in main areas of public space across Bournemouth, Poole and Christchurch is established on the principles of The Data Protection Act (GDPR/DPA) 2018 with the purpose of "Crime Prevention and Detection and the Apprehension and Prosecution of Offenders".

The two essential purposes to establish the lawful use of CCTV is: -

- A legal requirement
- Compliance with the Data Protection Principles

Local authorities establish their CCTV systems under the GDPR/DPA 2018 and Section 17 Crime and Disorder Act 1998 which places an obligation on local authorities and the police to work in partnership to develop and implement a strategy for tackling crime and disorder.

Section 17 outlines how and why local services may impact on crime and disorder and indicates the reasonable actions that might be put in place to ensure a co-ordinated approach to crime reduction. Evidence shows the opportunity for crime and disorder may be reduced and the safety and reassurance of the public improved when there is adequate CCTV coverage and it is used with other interventions. Using CCTV remains a strategic, financial and operational choice in exercising crime reduction partnership responsibilities between the police and other relevant supporters. In addition, 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.

Public support for the use of CCTV is still popular and accepted but it may be regarded by some as an infringement of peoples' liberty. To retain the respect and support of the general public, CCTV must be used fairly, in accordance with current laws and with the utmost integrity at all times. CCTV operations must stand up to scrutiny and be accountable to the communities and people they are aiming to protect.

1.2 The BCP Council Public Space CCTV System

The BCP Council public space CCTV System comprise a range of cameras installed at various strategic locations throughout the town including streets, parks, public places, car parks and Council premises. The cameras offer full colour, pan, tilt and zoom (PTZ) capability, some of which may be automatically switched to compensate for low light conditions. The local authority has the capability to redeploy some of their CCTV cameras in order to respond to changing crime / disorder trends and justified community needs. The locations of CCTV cameras can be found in Appendix F and on the BCP website.

1.3 Objectives of the System

The BCP CCTV System operates for the following purposes or objectives:

1. To help prevent, detect and reduce crime, disorder, public nuisance and anti-social behaviour including drug and alcohol related violent crime

2. To reduce any apprehension of crime, anti-social behaviour and aggression and provide reassurance for all those that live, work, trade and visit the area therefore enhancing community safety and boosting the economy

3. To assist statutory agencies (police, council etc.) to deploy their resources effectively

4. To assist in the management of the public areas covered by CCTV and support a local authority's civil enforcement and regulatory functions

5. To monitor traffic flow and assist in traffic management issues

6. Identify, apprehend and prosecute offenders in relation to crime, public order, road traffic accidents involving serious injury and all forms of harassment cases

7. To assist in civil emergencies and countering terrorism

8. To assist the emergency services in all aspects as appropriate, including major exercises relating to criminal activities and public safety

9. Provide the Police, the Council, and other authorised organisations with evidence upon which to take criminal and civil actions in the Courts including identifying witnesses

10. Promote the objectives of Dorset Police and Community Safety Partnership.

11. In appropriate circumstances, assisting the investigation of road traffic accidents.

The Council's Chief Executive or local police commander, after consultation, may draw up specific objectives based on local concerns. These will be documented, made available as necessary and reviewed periodically.

2. General Principles

2.1 The BCP Public Space CCTV System will at all times be developed, operated and managed in accordance with the following principles that are at the heart of this Code. Later sections will give specific information and guidance on key areas of operation.

1. The System will be operated with full regard for the principles of the Human Rights Act 1998; in particular that everyone has the right to respect for their privacy. This will include recognising peoples' rights to be free from degrading treatment and avoiding discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status. The operational procedures will ensure that evidence is kept securely and made available as required to ensure everyone's right to a fair trial in the event of any judicial proceedings or tribunal.

2. The System will be operated in accordance with the Data Protection Act/GDPR 2018 at all times and in particular the Information Commissioner's Code of Practice for CCTV. Systems will be operated fairly, within the law, and only for the stated purposes. Throughout this Code it is intended, as far as possible, to offer a balance between the purposes of CCTV and the need to safeguard the individual's right to privacy. (See Privacy and Data Protection; Section 3).

3. Occasionally the CCTV System may be required to assist with specific operations by law enforcement agencies. On every occasion appropriate authorisation for covert 'directed' surveillance will be obtained in accordance with the Regulation of Investigatory Powers Act 2000 (RIPA), Dorset Police (or the relevant agencies) policy and any existing guidance on the use of public space CCTV from the Investigatory Powers Commissioners Office (IPCO).

4. The decision to use, or the continued use of CCTV cameras and equipment will be supported by the SCC Self-Assessment Tool, Operational Requirement and the Data Protection Impact Assessments as required by the ICO. Where appropriate 'Privacy zones' may be technically applied to equipment to ensure privacy is protected in specific areas. Every use of CCTV will always be reasonable, necessary and proportionate. Wherever possible and appropriate, consultations with local communities and individuals on the general use of CCTV will be undertaken.

5. Public interest in the operation and management of CCTV will be recognised by ensuring the security and integrity of all personal information and operating procedures.

6. Participation in the System by any local organisation, individual or authority assumes an agreement by all participants to comply fully with and to be accountable under the Code of Practice.

7. Any major changes to the Code will only take place after consultation with all relevant interested parties in the operation of the System. Minor changes may be agreed between the persons nominated in **Appendix A**.

2.2 Home Office Surveillance Camera Code of Practice 2013

Our Code of Practice reflects the 12 Guiding Principles listed in the Home Office Surveillance Camera Code of Practice 2013.

- 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.
- The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
- There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
- There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
- 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.
- 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.
- 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.
- 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.
- Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
- 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.
- 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.
- 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.

The System is certified against the SCC Code of Practice.

3. Privacy and Data Protection

3.1 Public Concern

CCTV surveillance has become a common feature of our daily lives. Whilst the use of CCTV continues to enjoy general public support, it necessarily involves intrusion into the lives of ordinary individuals as they go about their day to day business. Those who express concern do so mainly over matters relating to the processing of the information, (or data) i.e. who is watching, why and what happens to the images.

The Human Rights Act 1998 affects many aspects of CCTV operations by public bodies, particularly respect for everyone's right to their private and family life and their home, (Privacy) and evidence management for the right to a fair trial.

The transmission, capture, retention, storage and disclosure of personal data by the BCP CCTV System will be strictly in accordance with the requirements of the GDPR/DPA 2018.

The Code is intended, as far as possible, to balance the objectives of the System with the need to safeguard the individual's rights. Every effort has been made throughout the Code to indicate that a formal structure has been put in place, including a complaints procedure, by which it can be identified that the System is not only accountable, but is seen to be accountable.

Security of all data will remain paramount. Maintaining public trust and confidence in the use of CCTV is essential if its benefits are to be realised and its use is not to become increasingly viewed with suspicion.

None of the cameras forming part of the System are, or shall be, installed or operated in a covert manner. The location of any camera is not intended to be covert. Cameras will not be concealed from the view of any person likely to be within the field of view of that camera. No dummy cameras are, or shall be, installed as part of the System.

The Criminal Procedures and Investigations Act 1996 introduced a statutory framework for the disclosure to defendants of material, which the prosecution would not intend to use in the presentation of its case (known as unused material).

3.2 Data Protection information

The Data Controller for the CCTV System is the Data Protection Officer for BCP Council. The day-to-day responsibility for the data will be devolved to the CCTV Manager or his nominated deputy.

All data will be processed in accordance with the principles of the GDPR/DPA 2018 which, in summarised form, includes, but is not limited to:

1. All personal data will be processed fairly and lawfully
2. Personal data will be only be held for the purposes specified in Section 3 of this Code
3. Personal data will only be used for those purposes, and only disclosed in accordance with this Code and operational procedures
4. Personal data will only be held which are adequate, relevant and not excessive in relation to the purposes specified
5. Steps will be taken to ensure that all personal data is accurate and where necessary, kept up to date
6. Personal data will not be held for longer than is necessary (typically 31 days unless data is required as evidence)
7. Individuals will be allowed access to their own personal information in a form they can read and, where appropriate, permitted to correct or erase it. (See Section 8.3 of the Code for details)
8. Security procedures will be implemented to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of, personal information
9. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal Data

The BCP public space CCTV System will at all times use every effort through prompt fault reporting in accordance with maintenance agreements to ensure all CCTV equipment is maintained 'fit for purpose' as required by GDPR/DPA 2018.

The BCP public space CCTV System is fully compliant with the Information Commissioner's Code of Practice for CCTV and will conduct CCTV operations in accordance with its guidance. The full ICO CCTV Code can be obtained from the website www.ico.gov.uk.

A summary of the key areas of compliance with the ICO Codes of Practice for CCTV is included in this Code at **Appendix B**.

4. Staffing of the CCTV Control Rooms

4.1 General

The CCTV Control Room will only be staffed by trained operators in accordance with local policies and operational procedures.

Staffing will always be in accordance with the Operational Procedural Manual. Regardless of staffing, the System will continuously record camera views at all times.

All staff will be fully conversant with this Code and their procedures which they will be expected to comply with as far as reasonably practicable at all times.

4.2 Private Security Industry Act 2001 and the Security Industry Authority (SIA)

Under the provisions of the Private Security Industry Act 2001 it is a criminal offence for staff to be 'contracted' as public space surveillance (CCTV) operators in England, Wales and Scotland without an SIA licence. The Security Industry Authority is the organisation responsible for regulating the private security industry. It is an independent body reporting to the Home Secretary under the terms of the Private Security Industry Act 2001. For more information visit: www.sia.homeoffice.gov.uk

A Public Space Surveillance (CCTV) licence is required when activities ('licensable duties') are carried out through the use of CCTV equipment to:

a) monitor the activities of a member of the public in a public or private place

or

b) identify a particular person(s)

A Public Space Surveillance (PSS - CCTV) licence is only required when services are supplied for the purposes of or in connection with any contract to a consumer.

Contracted staff operating in the CCTV Control Room will be in possession of an SIA CCTV Licence in compliance with this legislation as necessary. Only warranted police officers are exempt under the provisions of the Private Security Industry Act 2001.

4.3 Staff Vetting

It will be a condition of employment that all staff being selected for a role in the CCTV Control Room are successful through locally agreed vetting procedures and those defined by the SIA where a CCTV Licence is required.

As an 'Airwave' Police Digital Radio is installed, staff will be vetted to Non-Police Personnel standard as required by the College of Policing and Dorset Police.

4.4 Staff Training

Every member of staff directly connected to the operation of CCTV or with responsibility for the Control Room will be trained appropriately for their role.

As a minimum the Information Commissioners CCTV Code requires all staff to be trained in their responsibilities for data management.

All operators will be required to undergo formal training with regard to their responsibilities with regard to Confidentiality, GDPR/DPA, HRA and RIPA (the Regulation of Investigatory Powers Act).

4.5 Discipline

Every individual with any responsibility under the Operational Procedural Manual or the terms of this Code and who has any involvement with the Systems to which they refer, will be subject to their employer's disciplinary policy or procedures. Any breach of the Code or of any aspect of confidentiality may/could be dealt with in accordance with those disciplinary rules. A breach of the Code may result in criminal proceedings.

4.6. Making Enquiries or Complaints about CCTV

A member of the public wishing to make enquires or a complaint about any aspect of the BCP public space CCTV System may do so by contacting the system manager.

All complaints will be treated seriously. They will be dealt with in the same way as the discipline and complaints procedures which apply to all staff of the Council and Dorset Police staff. Copies are available from the respective organisations.

The CCTV system manager will ensure that every complaint is acknowledged in writing which will include advice about the procedure to be undertaken. Details of all complaints and the outcome will be included in the regular reports supplied by the System Manager and included in the Council's annual report.

If the outcome from a complaint about how the System operates or how images (data) were handled is thought to be unsatisfactory, the Office of the Information Commissioner will investigate independently. Individuals have additional rights under DPA to prevent processing likely to cause substantial and unwarranted damage or distress and to prevent automated decision-taking in relation to the individual.

Visit www.ico.gov.uk ; telephone 01625 545745 or write to:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

5. CCTV Control Room Access and Security

5.1 Authorised Access

To ensure security and confidentiality of the information processed (data) by the public space CCTV System, access to the CCTV Control Room is restricted. Entry will not be allowed without proper and sufficient reason and will at all times be in accord with the stated purposes of CCTV.

Regardless of status of the person(s), all access to the Control Room (and the information contained within) will be recorded in a Visitors Log. All visitors will be reminded of their obligation to confidentiality by displayed notices and a clause in the Visitors Log.

Those with day-to-day responsibility for operating the CCTV Systems will ensure only authorised access and an accurate visitors log is maintained and enforced.

5.2 Public Access

Access to the Control Room is restricted. However, in the interest of openness and accountability, anyone wishing to visit may be permitted to do so, subject to the approval of:

- A representative of the System owners (See Key Personnel at **Appendix A**) or
- The Control Room Supervisor

Public access must be for lawful, proper and sufficient reasons and only with approval. The CCTV staff must always be aware of public visits in advance and the visits may be terminated for operational reasons at the discretion of the CCTV Operator. All public visits will be conducted and recorded in accordance with the Operational Procedural Manual.

5.3 Security

Authorised personnel will be present at all times when the equipment is in use. If the Control Room is 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 Operational Procedural Manual will be complied with.

6. Operation and Management of the CCTV Systems

6.1 General

All the equipment associated with the System will only be operated by authorised personnel who have been properly trained in its use and in accordance with local operating procedures. Any person authorised to operate the cameras will always act with utmost probity.

The operator's role is to monitor, identify and respond to incidents. The cameras will only be used for the purposes stated and will not be used to look into private property or residences. Electronic 'privacy zones' may be used to ensure that the interior of any residence or private property within range of the System cannot be viewed. Staff training in privacy issues will always be given.

The operators will abide by the Human Rights Act and may be required to justify their monitoring or recording of any persons, activity or property at any time.

Records of operators on duty in the control room and those operating the cameras will be maintained. Each operator will 'log on' and 'off' the CCTV control system to ensure and audit trail of the operator who controls the cameras is retained and accurate.

The CCTV management software will enable supervisors and managers to interrogate the use and the records created on the CCTV system in order to compile the results of the use and incidents recorded.

From time to time arrangements may be made for Council or police staff to be present in the Control Room to support CCTV operations. These staff will be made aware of the provisions in this Code and their presence will be in accordance with the Operational Procedural Manual.

6.2 Signs

Signs will be placed in the areas covered by cameras to make the public aware of CCTV surveillance. The signs will indicate:

- The presence of CCTV monitoring (typically using a graphic of a CCTV camera)
- The 'ownership' of the System
- A contact telephone number and website address for further information
- A summary of the purpose of the surveillance will also be included.

6.3 Transmission, Recording and Storing of CCTV Images

The cameras transmit images to the Control Room using a variety of methods. These include fibre-optic, twisted pair and coaxial cables, wireless and network technologies using secure transmission protocols via the internet. The integrity of transmission remains paramount and every effort is to be made to maintain security.

The methods used will either be owned by the individual System or provided under contract by an industry supplier.

The Control Room uses Digital Video Recorders (DVR's) to record the images from all cameras simultaneously throughout every 24-hour period. The DVR's are housed securely in the Control Room equipment rack. Recorded images are retained on the DVR's for 31 days.

At the end of this retention period the recorded images are erased using the continual automatic digital process of 'overwriting'. This meets the requirements of not keeping data for longer than necessary; a principle of data processing. Only the DVR equipment housed within the Control Room record images from any of the cameras.

Recorded images can be replayed on dedicated computer workstations in a secure area and on the operator workstations. Only authorised staff and police officers can produce hard copies of recorded images (e.g. exporting onto disk - DVD-R) when required for proper purposes, i.e. evidence for court proceedings, investigation of alleged offences. In these circumstances the selected images will be kept for longer in accordance with the rules of evidence and the Operational Procedural Manual.

All recording, viewing and exporting equipment will only be operated by trained and authorised users. Members of the public must have total confidence that information recorded by the CCTV System will be treated with integrity, security and respect for their privacy.

6.4 Audit Trail (Record keeping)

There will be records kept, either paper-based or electronically on a computer, of all relevant activity 24/7. This is known as log-keeping or audit trail. This will typically include but not limited to:

- Staff duty times and breaks
- Visitors – name, times in/out and reasons for visit
- Actions taken by the operators and incidents reported to or seen by them
- Review and disclosure of CCTV images
- Faults reporting and rectification and the regular maintenance programme
- Security Staff Lone Worker Logs

Every CCTV recording or part of the audit trail has the potential of containing 'material' that may be required as evidence at some point. For the purposes of the Code 'material' means any material created or recorded by CCTV staff or CCTV equipment as part of operational procedure and specifically includes CCTV recordings, copies of them (including video/paper prints) and paper or electronic records.

All record keeping will be carried out in accordance with local operating procedures.

6.5 Evaluation

The System shall be periodically evaluated to establish whether the purposes of the System are being compiled with and whether objectives are being achieved. The evaluation shall include:

- An assessment of the impact upon crime. This assessment shall include the immediate area covered by the cameras and also the wider town area, the police divisional and regional areas and national trends
- An assessment of the incidents monitored by the System
- An assessment of the impact on town centre business
- An assessment of neighbouring areas without CCTV surveillance
- The views and opinions of the public
- The operation of the Code
- Whether or not the purposes for which the System was established are still relevant
- Cost effectiveness

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

6.6 Operation of the System by the Police – RIPA

Under certain operational circumstances, the police may make a request to assume direction of the System. These circumstances may be a major incident or event that has significant impact on the prevention and detection of crime or on public safety. Such use will provide the police with a broad overview of events in order to manage the incident.

Such requests to use the System's cameras will be dealt with individually and with due regard to the requirement for authority for specific types of surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA) (**see Appendix F**).

Requests made above will be considered on the written authority of a police officer of Superintendent rank or above to the System Manager. Any such request will be subject to the written authority of the Nominated Representative or their designated deputy. In the event of urgency, the verbal authority of the senior officer in charge, and in any event an officer not below the rank of Inspector, will be necessary and must be followed as soon as reasonably practicable, or in any event within 72 hours, by a Superintendent's written authority.

In the event of such a request being permitted, the Control Room will continue to be staffed and the System operated only by those personnel who are trained and authorised to do so and who fall within the terms of this Code.

In very extreme circumstances a request may be made for the police to take total exclusive control of the System, including of staffing of the Control Room and personal control of all associated equipment, to the exclusion of all representatives of the Owner. Any such request should be made to the System Manager in the first instance, who will consult personally with the Nominated Representative or their designated deputy. A request for total exclusive control must be made in writing by a police officer not below the rank of Assistant Chief Constable.

6.6.1 RIPA Authorisations by BCP Officers

It is the policy of BCP to nominate officers who can authorise RIPA surveillance on behalf of the Council e.g. Chief Executive, Strategic Directors and Heads of Service. The Council's Policies, Protocols and Procedures relating to RIPA are attached at **Appendix G**.

6.7 Secondary recording and monitoring

Secondary monitoring equipment is located at the Police Communication Centre, Winfrith. A specific CCTV monitor at the police HQ is able to view any one replicated image selected by the CCTV operators in the control room. The police are not able to control the movement of the camera, they can simply view the image presented. Secondary monitoring equipment is located a various on and offsite locations. All sites are secure with restricted access.

6.8 Maintenance of the System

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

The maintenance agreement will make provision for regular / periodic service checks on the equipment which will include cleaning of 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.

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

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

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 in the System.

It is the responsibility of the System Manager or his nominated representative to ensure that appropriate records are maintained in respect of the functioning of the cameras and the response of the maintenance contractor.

7. Viewing and Disclosure of CCTV Recordings

7.1 General

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

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

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

It is therefore of the utmost importance that irrespective of the means or format (e.g. paper copy, DVD or any form of electronic processing and storage) of the images obtained from the System, they are treated strictly in accordance with this Code, the Procedural Manual and the provisions of GDPR/DPA 2018 from the moment they are received by the monitoring room until final destruction. Every movement and usage will be meticulously recorded.

Access to and the use of recorded material will be strictly for those purposes defined in the Code.

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

7.2 ANPR

ANPR may be incorporated into the CCTV System for specific operational purposes at the discretion and approval of the Council. ANPR is owned by the Dorset Police and Dorset Police are responsible for the lawful processing of ANPR data. Where Dorset police wish to incorporate ANPR the Council will require a formal request by letter or e-mail from the Dorset Police stating the reason for the request and expected length of the operation.

7.3 Main Requests for Viewing and Disclosure

Requests for viewing and disclosure of CCTV information will normally be granted to organisations that show valid reasons which meet the stated purposes of CCTV. These are mainly (but not limited to) the following organisations:

- All UK police staff, (including Ministry of Defence and Military Police)
- Statutory authorities with powers to prosecute, (e.g. H.M. Revenue and Customs, councils, Trading Standards, Environmental Health, etc.)

- Solicitors or their legal representatives in criminal or civil proceedings; (such a request may incur a fee)

- Individuals representing themselves in judicial proceedings

- Other agencies (e.g. Insurance companies) according to purpose and legal status. A fee may be incurred

7.4 Schedule 2 GDPR/DPA 2018

The listed GDPR provisions do not apply to personal data consisting of information that the controller is obliged by an enactment to make available to the public, to the extent that the application of those provisions would prevent the controller from complying with that obligation.

The listed GDPR provisions do not apply to personal data where disclosure of the data is required by an enactment, a rule of law or an order of a court or tribunal, to the extent that the application of those provisions would prevent the controller from making the disclosure.

The listed GDPR provisions do not apply to personal data where disclosure of the data— (a) is necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings), (b) is necessary for the purpose of obtaining legal advice, or (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights, to the extent that the application of those provisions would prevent the controller from making the disclosure.

7.5 Criminal Procedures and Investigations Act, 1996

The Criminal Procedures and Investigations Act, 1996 provides a legal framework for the disclosure to accused persons of material gathered during the course of an investigation. All agencies with responsibilities for investigating offences which may lead to proceedings in the criminal courts have to comply with the requirements.

Disclosure of material under the provisions of this Act (for the prosecution and defence of an alleged criminal offence) should not be confused with the rules of 'Subject Access' disclosure by the Data Protection Act 2018.

7.6 Freedom of Information Act 2000

The Freedom of Information Act (FOIA) deals with access to official information held by most public authorities (police or councils, etc.). It also applies to companies which are wholly owned by public authorities.

The Act gives the public a general right of access to information held by public authorities; typically, around decisions, statistics, spending money and effectiveness. Requests may be

by letter or email. The public authority must state whether it holds the information and normally supply it within 20 working days in the format requested.

When responding to requests, there are procedural requirements set out in the Act which an authority must follow. There are also valid reasons for withholding information, which are known as exemptions from the right to know.

FOIA exemptions apply to disclosure of CCTV images:

- If the images are those of the FOIA requester then that information will be treated as a Subject Access request as explained at 7.3 of this Code

- If the images are of other people/vehicles etc., these can only be disclosed if disclosing the information in question does not breach the data protection principles

In practical terms, if individuals are capable of being identified from the relevant CCTV images, then it is personal information about the individual concerned. It is unlikely that this information can be disclosed in response to an FOIA request. The requester could potentially use the images for any purpose and the individual concerned is unlikely to expect this and likely to be unfair processing breaching the Data Protection Act (DPA).

This guidance is not exhaustive and full information on FOIA issues can be found at www.ico.gov.uk.

7.7 Release of Data to a Third Party

Every request for the release of Personal Data generated by the System will be channelled through the System Manager or his authorised representative. The System Manager will ensure that the Good Practice Principles contained within Appendix C to the Code are followed at all times. Requests for access will be dealt with in accordance with the Council's GDPR/DPA 2018 procedures. Information for individuals about how to make a request for access to their Personal Data is available on the Council's website.

Applicants will not be permitted to view recorded information within the CCTV Control Room, but may be offered the opportunity to view the images recorded of them in suitable Police or Council accommodation made available to facilitate this where this is practicable and possible. 'Suitable' means private and not overlooked.

In complying with the Good Practice Principles for the release of Personal Data to third parties it is intended, as far as reasonably practicable, to safeguard the individual's right 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.

- Access to recorded material will only take place in accordance with the standards outlined in Appendix C to the Code.

- The release or disclosure of Personal Data for commercial or entertainment purposes is specifically prohibited.

Members of the Dorset Police or other agency having statutory authority to investigate and/or prosecute offences may, subject to compliance with Appendix C, release details of recorded information to the media where this reasonably required to assist in the identification of alleged offenders or potential witnesses.

Full details of any recorded information originating from the System in whatever format for release to the media by the Dorset Police must be recorded and permission must be obtained from the System Manager prior to the release of any such material.

7.8 Retention of footage and Recording Media

Footage will be retained on the System hard drive for a minimum of 31 days, after which the data will be overwritten. Footage will be held 'on request' in the council evidence locker for 31 days, after which it will be deleted from the system.

Only the Owner's discs will be used. The Owner will not retain any copies. The CCTV Liaison Officer or Investigating Officer will seize the 'Master disc'. Any further copies will be made by the police. Discs that are retained in the Control Room for collection by the investigating officer will be reviewed periodically. If they are not collected within 12 months they will be destroyed. Once the Master discs have been seized by the investigation officer that officer assumes ownership of the data (becomes the Data Controller) and is responsible for its security, evidential continuity and eventual destruction when it is no longer required. Dorset Police become the Data Controller when any other data is transferred to their possession and control, for example video print or transfer of video footage into the 'evidence locker'**.**

Each disc will have a unique tracking record maintained in accordance with the Procedural Manual. The tracking record shall identify when the disc has been used, for which incident and the details of the investigating officer requesting the footage. All such records will be held on the Owner's management reporting system.

Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24-hour period in real-time and time-lapse mode.

Appendix A Key Personnel and Responsibilities

1. System Owner

BCP Council

Tel. 01202 451451

BCP Council is the Owner of the System. The Head of Community Safety is the Nominated Representative on behalf of the Owner whose role will include responsibility to:

i) Ensure the provision and maintenance of all equipment forming part of the System in accordance with contractual arrangements, which the owner may from time to time enter in to.
ii) Maintain close liaison with the System Manager.
iii) Ensure the interests of the Community Safety Partnership are upheld in accordance with the terms of the Code.
iv) Authorise proposed alterations and additions to the System, the Code and the Procedural Manual.

2. System Management

CCTV Control Room
BCP Council
Dorset Police
Bournemouth Divisional HQ
Madeira Road
Bournemouth
BH1 1QQ
Tel. (01202) 222002

Responsibilities

The Owners will employ a dedicated System Manager. The System Manager will have delegated authority for data control on behalf of the Data Controller. This role includes responsibility to:

I. Maintain day to day management of the System and CCTV Operators.

II. Accept overall responsibility for the System and for ensuring that the Code and requirements of the Procedural Manual are complied with.

III. Maintain direct liaison with the Nominated Representative.

IV. Maintain direct liaison with the Partnership partners.

Roles and Relationships

BCP Council and Dorset Police

BCP Council owns the CCTV Community Safety System. However, for the purposes of the GDPR/DPA 2018, both the Council and Dorset Police are the Data Controllers and have joint legal responsibility for the processing of information associated with the System. Both the

Council and Dorset Police are also responsible for ensuring that the operation of the System complies with the Human Rights Act (HRA) and the common law duty of confidentiality. The Council and Dorset Police will work in partnership to achieve the purposes and objectives of the System, Code and the Information Sharing Agreement (ISA).

Other Non-Council CCTV System Owners (additional systems)

Owners of these additional systems may be granted approval to connect to the Council's System in accordance with Section 8 of the Code. The owners of such additional systems shall be Data Controllers for the purposes of the GDPR/DPA 2018 and the Council is the Data Processor. A legally binding contract will be in place between the Council (Data Processor) and the owners of these additional systems (Data Controller) in each case. If owners of additional systems wish to enter into partnership with Dorset Police they will be required to have their own Information Sharing Agreements (ISAs) in place. The Council as the Data Processor will only disclose CCTV information to Dorset Police in accordance with the terms & conditions of their ISA.

CCTV Strategy Group

The CCTV Strategy Group is a partnership group comprising Council and Dorset Police officers. The Group will:

1. Monitor practice against this Code, the Procedural Manual and the ISA.
2. Review and update the Code and the ISA on an annual basis.
3. Make decisions on strategic policy issues, as and when they arise. This will ensure that the agreed aims and objectives set out in the Code continue to be met.
4. Ensure that the public are adequately informed about the purpose, management and operation of the Council's CCTV System.
5. Make decisions with regard to the disclosure of CCTV information in response to specific requests from third parties (including the media), where such requests have the potential to adversely impact on either the Council or the Dorset Police.
6. Make decisions on requests for new/additional cameras to take into account the evidence of need (operational requirement), privacy impact and funding. The strategy group will also undertake to ensure public consultation is carried out before the installation of any new permanent cameras where there is any likelihood that this may impact on the privacy of individuals.
7. Investigate any reported matters of a serious nature relating to non-compliance with this Code, the ISA, or breaches of confidentiality or the DPA and take appropriate action.

The Council's CCTV System Manager

The Council's CCTV Manager is responsible for the integrity, security, procedural efficiency and methods of operation of the System, including the gathering, retention and release of CCTV data.

This will include:

1. Management and training of CCTV Operators and any other Dorset Police or Council officers authorised to assist in the operation of the System;
2. The disclosure of information to the Dorset Police in accordance with the Information Sharing Agreement between the Dorset Police and the Council;

3. Release of information to other third-parties who have a legal right to such information;

4. Access to the Control Room including:
    - control and security clearance of visitors
    - security and storage of information
    - security clearance of persons who are permitted to view information;
5. Release of new, and destruction of old data, and data medium;
6. Maintenance of the quality of the recording and monitoring equipment.

The Council's CCTV Manager will work in partnership with the Police CCTV Liaison Officer with regard to the disclosure of information to the Dorset Police for the purposes defined in the ISA. The Council's CCTV Manager will consult with the Police CCTV Liaison Officer in respect of any procedural or operational matters connected with the viewing or release of information to the Dorset Police.

Dorset Police (BCP Area) CCTV Liaison Officer

The Dorset Police CCTV Liaison Officer is responsible for the integrity, security, procedural efficiency and methods of operation of the System.

The Dorset Police CCTV Liaison Officer is responsible for managing all Dorset Police requests for the disclosure of information from the Council's CCTV System and is the single point of contact between the Dorset Police and the Council for this purpose. The Dorset Police CCTV Liaison Officer will at all times adhere to the requirements of this Code and the ISA. The Dorset Police CCTV Liaison Officer will promote good practice by ensuring that Dorset Police Officers seeking the disclosure of CCTV information are aware of this Code and the ISA and follow agreed procedures.

CCTV Operators

The CCTV Operators are responsible for the integrity, security, procedural efficiency and methods of operation of the System.

Council contracted CCTV Operators will be trained and possess a CCTV SIA licence.

CCTV Operators will not use equipment for purposes other than those intended and will comply with the relevant legislation outlined in this code and the Procedural Manual. They shall be mindful at all times to avoid exercising prejudices that may lead to complaints about the System.

All CCTV Operators contracted will be subject to the contractor's disciplinary procedures in matters relating to non-compliance with this Code or the Procedural Manual, breaches of confidentiality, or the unauthorised release of data.

All CCTV Operators employed by the Council will be subject to the Council's disciplinary procedures in matters relating to non-compliance with this Code or the Procedural Manual, breaches of confidentiality, or the unauthorised release of data.

Appendix B GDPR & DPA 2018

Copies of the Act and the Information Commissioners Code of Practice can be downloaded from the website:

www.ico.gov.uk

Appendix C Good Practice for the Release of Data to Third Parties

1. Introduction

Arguably CCTV is 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. Owners and managers of such systems are to command the respect and support of the general public, the systems must not only be used with the utmost probity at all times, they must be used in a manner which stands up to scrutiny and is accountable to the very people they are aiming to protect.

The BCP Council is committed to the belief that everyone has the right to respect for his or her private and family life and their home. Although the use of CCTV 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 information (data) which the system gathers.

After considerable research and consultation, the Owners have adopted the Good Practice Principles developed by The CCTV User Group.

2. General Policy

All requests for the release of data shall be processed in accordance with the Procedural Manual. All such requests shall be channelled through the Data Controller.

Note: *The data controller is the person who (either alone or jointly with others) determines the purpose for which and the manner in which any Personal Data are, or are to be processed.*

Day to day responsibility has been devolved to the System Manager.

3. Primary Request to View Data

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

   i) Providing evidence in criminal proceedings (e.g. Police and Criminal Evidence Act 1984, Criminal Procedures & Investigations Act 1996, etc.)
   ii) Providing evidence in civil proceedings or tribunals
   iii) The prevention of crime
   iv) The investigation and detection of crime (may include identification of offenders).
   v) Identification of witnesses

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

   i) Police *(see note 1)*
   ii) Statutory authorities with powers to prosecute (e.g. Custom & Excise, Trading Standards, etc.)
   iii) Solicitors *(see note 2)*
   iv) Plaintiffs in civil proceedings *(see note 3)*
   v) Accused persons or defendants in criminal proceedings *(see note 3)*
   vi) Other agencies, according to purpose and legal status *(see note 4)*

c) Upon receipt from a third party of a bona fide request for the release of data, the data controller shall:

i) Not unduly obstruct a third-party investigation to verify the existence of relevant data.
ii) Ensure the retention of data which may be relevant to the request, but which may be pending application for, or the issue of, a court order or subpoena. A time limit shall be imposed on such retention, which will be notified at the time of the request.

d) In circumstances outlined in note (3) below, (requests by plaintiffs, accused persons or defendants) the data controller, or nominated representative shall:
i) Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation.
ii) Treat all such enquiries with strict confidentiality.

Notes:

1) *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, Military Police, etc. (Special arrangements may be put in place in response to local requirements)*

2) *Aside from criminal investigation, 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.*

3) *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.*

4) *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.*

5) *The data controller can refuse an individual request to view if sufficient or inaccurate information is provided. A search request should specify reasonable accuracy (could be specified to the nearest half-hour).*

4. Secondary Request to View Data

a) 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:
i) The request does not contravene and that compliance with the request would not breach current relevant legislation, (e.g. GDPR/DPA 2018, Human Rights Act 1998, Freedom of Information Act 2000, section 163 Criminal Justice and Public Order Act 1994, etc.);
ii) Any legislative requirements have been complied with (e.g. the requirements of the GDPR/DPA 2018, Freedom of Information Act 2000);
iii) Due regard has been taken of any known case law (current or past) which may be relevant (e.g. R v Brentwood BC ex p. Peck) and

iv) The request would pass a test of 'disclosure in the public interest' (see note 1).

b) 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 to place before releasing the material:
   i) 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 the CCTV Code of Practice.
   ii) If the material is to be released under the auspices 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 the CCTV Code of Practice.

Notes:

'Disclosure in the public interest' could include the disclosure of Personal Data that:

i) provides specific information which would be of value or of interest to the public well being
ii) identifies a public health or safety issue
iii) leads to 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 (see 3 above).

5. Individual Subject Access under GDPR/DPA Legislation

a) Under the terms of the GDPR/DPA legislation individual access to Personal Data, of which that individual is the data subject, must be permitted providing:
   i) The request is made in writing
   ii) There is no fee is paid for each search
   iii) A data controller is supplied with sufficient information to satisfy him/herself as to the identity of the person making the request.
   iv) The person making the request provides sufficient and accurate information about the time, date and place to enable the data controller to locate the information which that person seeks (it is recognised that a person making a request may not know the precise time. Under those circumstances it is suggested that within one hour of accuracy would be a reasonable requirement)
   v) The person making the request is only shown information relevant to that particular search and which contains Personal Data of him/herself only, unless all other individuals who may be identified from the same information have consented to the disclosure.

b) 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).

c) 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 treated on its own merits.

d) In addition to the principles contained within the Data Protection legislation, the data controller should be satisfied that the data is:
   i) Not currently and as far as can be reasonably ascertained, not likely to become part of a 'live' criminal investigation.
   ii) Not currently and as far as can be reasonably ascertained, not likely to become relevant to civil proceedings
   iii) Not the subject of a complaint or dispute which has not been actioned
   iv) The original data and that an audit trail has been maintained
   v) Not removed or copied without proper authority
   vi) For individual disclosure only (i.e. to be disclosed to a named subject)

6. Process of Disclosure

a) Verify the accuracy of the request.
b) Replay the data to the requester only (or responsible person acting on their behalf).
c) The viewing should take place in a separate room and not in the control room or monitoring area. Only data relevant to the request to be shown.
d) 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.
e) If a copy of the material is requested and there is no on-site means of editing out other Personal Data, then the material shall be sent to an editing house for processing prior to being sent to the requester.

Note: *The Information Commissioners Code of Practice for CCTV makes specific requirements for the precautions to be taken when images are sent to an editing house for processing.*

7. Media Disclosure

7.1 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:
   i) 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.
   ii) The release form shall state that the receiver must process the data in a manner prescribed by the data controller, e.g. specific identities/data that must not be revealed.
   iii) It shall require that proof of any editing must be passed back to the data controller, either for approval or final consent, prior to its intended use by the media (protecting the position of the data controller who would be responsible for any infringement of Data Protection legislation and the System Code of Practice).
   iv) The release form shall be considered a contract and signed by both parties (see note 1).

Note:

In the well-publicised case of R v Brentwood Borough Council, ex parte Geoffrey Dennis Peck, (QBD November 1997), the judge concluded that by releasing the video footage, the Council had not acted lawfully. A verbal assurance that the broadcasters would mask the identity of the individual had been obtained. Despite further attempts by the Council to ensure the identity would not be revealed, the television company did in fact broadcast footage during which the identity of Peck was not concealed. The judge concluded that tighter guidelines should be

considered to avoid future accidental broadcasts. Attention is drawn to the requirements of the Information Commissioners in this respect, detailed in his Code of Practice summarised above.

8. Principles

In adopting these principles 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:

a) Recorded material shall be processed lawfully and fairly and used only for the purposes defined in the Code of Practice for the system.
b) Access to recorded material shall only take place in accordance with this standard and the Code of Practice.
c) The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

Appendix D

Subject Access Request Form

BCP COUNCIL CCTV SURVEILLANCE SYSTEM

GDPR/DPA 2018

These can be found online at:

http://www.bournemouth.gov.uk/PeopleLiving/CrimeDisorder/CCTV-Applicationformforaccess-Bournemouth.doc

Or by writing to:

CCTV Manager
BCP Council
Bournemouth Divisional Headquarters
Madeira Road
Bournemouth
BH1 1QQ

Appendix E Regulation of Investigatory Powers Act 2000 Guidance to CCTV Users

Introduction

Background

General observation forms part of the duties of many law enforcement officers and other public bodies. Police officers will be on patrol at football grounds and other venues monitoring the crowd to maintain public safety and prevent disorder. Officers may also target a crime 'hot spot' in order to identify and arrest offenders committing crime at that location. Trading Standards or HM Customs & Excise officers might covertly observe and then visit a shop as part of their enforcement function to verify the supply or level of supply of goods or services that may be liable to a restriction or tax. Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve **systematic surveillance of an individual.** It forms part of the everyday functions of law enforcement or other public bodies. This low-level activity will not usually be regulated under the provisions of the 2000 Act.

Neither do the provisions of the Act cover the normal, everyday use of **overt** CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime. *However*, it had not been envisaged how much the Act would impact on specific, targeted use of public/private CCTV Systems by 'relevant Public Authorities' covered in Schedule 1: Part 1 of the Act, when used during their planned investigations.

The consequences of not obtaining an authorisation under this Part may be, where there is an interference by a public authority with Article 8 rights (invasion of privacy), and there is no other source of authority, that the action is unlawful by virtue of section 6 of the Human Rights Act 1998 (Right to Fair Trial) and the evidence obtained could be excluded in court under Section 78 Police & Criminal Evidence Act 1978.

The Act is divided in to five parts. Part II is the relevant part of the Act for CCTV. It creates a system of authorisation for various types of covert surveillance. The types of activity covered are 'intrusive surveillance' and 'directed surveillance'.

'Covert Surveillance' defined:

Observations which are carried out by, or with, the use of a surveillance device. Surveillance will be covert where it is carried out in a manner calculated to ensure that the person or persons subject to the surveillance are **unaware** that **it is, or may be**, taking place.

Part II – Surveillance types

We should clearly differentiate in this guidance between 'intrusive' surveillance which will be a great rarity for CCTV operations and 'directed' surveillance which will be the more likely.

Intrusive Surveillance

This is a highly invasive type of covert surveillance; the like of which CCTV equipment and their images alone would not be able to engage in except on the most rare occasion. The Act states:

'Intrusive surveillance' is defined as covert surveillance carried out in relation to anything taking place on residential premises or in any private vehicle.

This kind of surveillance may take place by means either of a person or device located ***inside*** *residential* ***premises*** *or a private* ***vehicle*** *of the person who is subject to the surveillance, or by means of a device placed outside which* ***consistently provides a product of equivalent quality and detail as a product which would be obtained from a device located inside****.*

Therefore, it is **not intrusive** *unless* the camera capabilities are 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.

Our CCTV cameras are deemed incapable of providing this level of detail so as to be considered 'intrusive' for the purposes of the Act. Current interpretations re sustained gathering of images of persons in a car, in a car park, dealing in drugs; being able to see clearly inside the car would not be considered 'intrusive' under the Act.

In particular the following extract from Section 4 of the Code prevents us from carrying out intrusion of premises with cameras. This section puts us in a strong position to resist the use of public cameras in this way by investigators:

Cameras will not be used to look in to private residential property. Where the equipment permits it 'Privacy Zones' will be programmed in to the system as required in order to ensure that the interior of any private residential property within range of the system is not surveyed by cameras. If such 'zones' cannot be programmed the operators will be specifically trained in privacy issues.

Directed Surveillance

This level of covert surveillance is likely to be engaged more by public/private CCTV users when they are requested by 'authorised bodies' (see later) to operate their cameras in a specific way, for a planned purpose or operation, where 'private information' is to be gained.

The Act states:
'**Directed surveillance'** is defined in Section 26 subsection (2) as **covert surveillance** that is undertaken in relation to **a specific investigation or a specific operation** *which 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 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.* – **(planned).**

In this section 'private information', in relation to a person, includes any information relating to his private or family life.

If a CCTV user is carrying out normal everyday observations by operating a particular camera to gain the best information, albeit it may not be the most obvious camera to use, or the nearest to the incident being observed, that use will not be deemed to be 'covert' under the terms of the Act. It is using modern technology to the advantage of the operator. It will

only be where CCTV cameras are to be used in a planned, targeted way to gain private information that the requirements of authorised directed surveillance need to be met.

If users are requested to operate their cameras as part of a planned operation where the subject is unaware that targeted surveillance is, or may be, taking place, 'private information' is to be gained and it involves systematic surveillance of an individual/s (whether or not the target of the operation) then a RIPA 'directed surveillance' authority must be obtained.

Authorisations:

Intrusive surveillance can only be 'authorised' by Chief Officers within UK police forces and H.M. Customs and Excise and is therefore irrelevant for any other authority or agency. It is an area of RIPA that CCTV users can largely disregard.

Those who can authorise covert surveillance for public authorities listed in Sch.1/Part1, in respect to directed surveillance are detailed in Article2/Part 1 – Statutory Instrument 2417/2000: The Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) Order 2000 and Statutory Instrument 1298/2002: The Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) (Amendment) Order 2002.

E.g.:

A Local Authority (within the meaning of section 1 of the Local Government Act 1999). The prescribed office as a minimum level of authority is:

Assistant Chief Officer; Officer responsible for the management of an investigation.

Police Forces – A police force maintained under section 2 of the Police Act 1996 (police forces in England and Wales). The prescribed level is a Superintendent; for urgent cases an Inspector.

The impact for staff in 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 be an immediate response to events or circumstances. In this case it would not require authorisation unless it were to continue for some time.

In cases where a pre-planned incident or operation wishes to make use of public/private CCTV for such monitoring, an authority will almost certainly be required from the appropriate person with the authorised agency.

The authority must indicate the reasons 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 purposes of protecting public health
f) for the purposes of assessing or collecting any tax, duty, levy or other position, contribution or charge payable to a government department; or
g) for any purpose (not falling within paragraphs (a) to (f) which is specified for the purposes of this subsection by an order made by the Secretary of State.

It should be noted, however, that some authorities can only use limited grounds, e.g. local authorities are restricted to ground (b) whereas the police can use grounds (a), (b), (c), (d) and (e).

Every RIPA authority must be thought through and the thought process clearly demonstrated and recorded on the application. Necessity and proportionality must be fully considered; asking the questions: “is it the only way?”, “what else have I considered?”. It should not be a repeat of principles – in order to prevent & detect crime or in the interests of public safety etc.

Whenever an authority is issued it must be regularly reviewed as the investigation progresses and it must be cancelled properly upon conclusion. The completion of these stages will be looked at during any inspection process.

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 and then later in writing using the forms.

Forms should be available at each CCTV monitoring centre and are to be included in the procedural manual and available from the CCTV User Group website.

Policing examples:

Inspector Authorisation – urgent request (up to 72 hours)

An example of a request requiring urgent Inspectors authority might be where a car is found in a car park late at night and known to belong to drugs dealers. The officers might task CCTV to watch the vehicle over a period of time (*no longer response to immediate events*) and note who goes to and from the vehicle (*sustained surveillance of individuals gaining private information*).

Superintendent Authorisation – non-urgent request

Where crime squad officers are acting on intelligence linked to a long term, planned operation and they wish to have a shop premise, which is suspected of dealing in stolen goods, monitored from the outside over a period of days.

No authorisation required

Where officers are on patrol and come across a local drug dealer sitting in the town centre/street. It would not be effective for them to remain in a shop doorway and wish to have cameras monitor them instead, so as not to divulge the observation taking place. *Response to immediate events.*

For access to all relevant information on this Act, including the Schedules and Statutory Instruments referred to in this guidance please visit:

www.homeoffice.gov.uk/crimpol/crimreduc/regulation/index.html