CORNWALL PUBLIC SPACE CCTV SYSTEMS

CODE OF PRACTICE
Version 2

Quality Assurance Control

Hard copies of the Code of Practice may be inspected at the offices of the eleven town councils or viewed on their respective websites, or on the Cornwall Council website.

Version	Date	Amended By:
Draft	March 11	David George
Version 1	September 2011	David George
Review and Minor Amendments	April 2012	David George
Review and Minor Amendments	September 2013	David George
Amend to a draft Code for use post April 2015	October 2014	David George
Draft updated to reflect new guidance	January 2015	David George
Draft updated to reflect project board changes	March 2015	Nathaniel Hooton and David George
Final draft	May 2015	Nathaniel Hooton and Zoe Gofton
Version 1.1	December 2017	Traci Parker
Version 1.2	February 2019	Sarah Kind
Version 1.3	September 2020	John Rickard and Sarah Kind
Version 2.0	April 2021	John Rickard

CONTENTS

INTRODUCTION

1.1 The Cornwall Closed Circuit Television Management Group (CCTVMG) was formed in 2015. By 2020, the partnership comprises of thirteen town councils and Cornwall Fire, Rescue and Community Safety Service (CFR&CSS), which is part of Cornwall Council. All cameras are linked to the Cornwall Council Emergency Centre and, from there, on to the CFR&CSS control room, where real-time active monitoring takes place. CCTVMG meets quarterly to receive management reports, and discuss all matters relating to the system operations. This group is chaired and administered by representatives of a different town each calendar year.

1.2 Principles

This Code of Practice is based upon the legislation, principles and guidance contained in the following documents:

The Human Rights Act 1998

The Data Protection Act 2018 and General Data Protection Regulations (GDPR)

Crime and Disorder Act 1998

The Protection of Freedoms Act 2012

The CCTV National Code of Practice 2008

The Surveillance Camera Code of Practice 2013

The Private Security Industry Act 2001

In The Picture: Data Protection Code 2014

The partnership recognises that public authorities and those organisations carrying out the functions of a public service nature are required to observe the obligations imposed by the Human Rights Act 1998. The partnership considers that the use of CCTV in the towns herein stated is a necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve public safety.

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. The Local Authorities and Police also consider it a necessary initiative towards their duty under the Crime and Disorder Act 1998.

The CCTV systems within the partnership shall be operated with respect for all individuals, recognising the right to be free from inhuman or 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. Further the System shall be operated in such a way as to avoid infringement of individual privacy, and this will be assured through the completion of Privacy Impact Assessments (PIAs).

A PIA is completed whenever a new camera is installed and all PIAs are updated no less than annually. PIAs are completed by a group including a representative from the relevant town council, a Cornwall Council Rep and CFR&CSS.

The partnership recognises that it is their responsibility to ensure that the scheme should always comply with all relevant legislation, to ensure its legality and legitimacy. The scheme will only be used as a proportional response to identified problems and be used only insofar as it is necessary in a democratic society, in the interests of:

- national security
- public safety
- the economic wellbeing of the are
- the prevention and detection of crime or disorder
- the protection of health and morals
- the protection of the rights and freedoms of others.

The Codes of Practice and observance of the Operational Procedures contained in the manual shall ensure that evidence is secured, retained and made available as required so that there is absolute respect for everyone's right to a fair trial.

1.3 The System

For the purpose of this document 'The System' includes all hardware and software installed and linked to the 'Control Room'.

Individual town/city councils (hereafter referred to as 'the councils') are System Operators (as defined in the Protection of Freedoms Act 2012). They own the equipment and hold the software licences in respect of cameras and ancillary hardware installed in their respective towns.

Cameras are distributed as follows:

Town	Number of Cameras
Bodmin	13
Camborne	7
Hayle	6
Helston	10
Penzance	18
Redruth	8
Truro	30
Falmouth	19
St Ives	6
Wadebridge	6
Penryn	4
Liskeard	8
Perranporth	8
TOTAL	143

A full list of camera locations can be seen at Appendix A.

The system consists of 143 fully controllable, pan, tilt, zoom (PTZ) colour cameras which operate and record 24 hours a day 365 days a year. Cameras are proactively monitored on a directed information led basis. No notice is given of when cameras are being proactively monitored.

Control and monitoring equipment is owned by Cornwall Council.
The monitoring of cameras takes place in the Cornwall Fire and Rescue Service Critical Control Centre and full capability is also available in Cornwall Council's Emergency Centre.

1.4 Monitoring and System Users

CCTV active monitoring services are contracted by the councils to Cornwall Fire, Rescue & Community Safety Service.

1.5 Partners

The operation of all aspects of the CCTV System(s) including compliance with this Code of Practice are overseen by a properly constituted and accountable Management Group (CCTVMG) made up of representatives from all participating councils and partner agencies/organisations. A full list of responsible parties can be found at Appendix B.

1.6 Ownership and Copyright of Recorded Material

All recorded material and copyright therein belongs to the individual council where CCTV images are recorded. The Data Owner for CCTV is therefore the individual town councils. Copyright and ownership of all material will remain with the Data Controller until such a time as it is released to a third party, when ownership by the Data Controller is dissolved.

No part of any material may be transmitted or reproduced in any form or by any means or stored in any way without the written consent of the data owner(s).

Consent to use or reproduce or store any material other than for purposes set out in this Code of Practice will be withheld, except in exceptional circumstances.

1.7 Roles and Responsibilities

CCTV Owner - The 'owner' is just that, they own the system. They employ the operating staff either directly or as through a third party contractual agreement. They often occupy the title of 'Data Controller' for the purposes of ICO registration.
In respect of the Cornwall CCTV Group, the town councils assume the roles of CCTV Owner and Data Controller.

CCTV Manager - The 'manager' oversees the system and causes the operational requirements to be identified. They are also responsible for the necessary services and administration procedures to be adopted to lawfully and effectively achieve the aim of the system. They are also commonly responsible for managing the employment of staff.

CCTV Supervisor - The 'supervisor' ensures that the system operates in accordance to the adopted procedures and registered 'purposes of use'. They may also be required to set shift patterns and be the front-line link between staff and management.

CCTV Operator - The 'operator' is the Data Processor – processing the data that the system obtains. This includes the operation of most of the equipment, including joysticks and cameras, but only certain 'operators' may be authorised to make 'copies' of data for evidential use.

2. PRINCIPLES AND PURPOSE

2.1 Principles

The system is operated in accordance with all the requirements and the principles of the Human Rights Act.

The operation of the System also recognises the need for formal authorisation of surveillance as required by the Regulation of Investigatory Powers Act 2000, in particular Part 2 of the Act, and the police force policy.

The System is operated in accordance with the General Data Protection Regulations, all times.

The System is operated fairly, within the law, and only for the purposes for which it was established and are identified within this Code, or which are subsequently agreed in accordance with this Code of Practice.

The System is operated with due regard to the principle that everyone has the right to respect for his or her private and family life and their home. Article Eight of the European Convention on Human Rights defines the guiding principle: "Everyone has the right to respect for his private and family life, his home and his correspondence." This is subject to the exceptions set out under Article 8(2), "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

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

Throughout this Code of Practice it is intended, as far as reasonably possible, to balance the objectives of the CCTV 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.

Participation in the 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 of Practice.

Participation in this system by all councils, authorities and named partners will depend upon their willingness to comply with this Code of Practice and to be accountable under this Code of Practice.

2.2 Purposes

The main purposes of the system are: -

- a reduction in the fear of crime and reassurance of the public
- to help secure a safer environment for those who live, work or trade in the areas and those who visit the areas covered by the system
- the detection, deterrence and prevention of crime including:

-providing assistance in the prevention of crime

-deterring and detecting crime

-helping to identify, apprehend and prosecute offenders

-providing the Police with evidence to take criminal action in the Courts

-protecting vulnerable persons in the community

-the maintenance of public order

-as a tool in aspects of traffic management

-contributing to improvements to the Town Centre environment

2.3 Key Objectives

The key objectives of the system are: -

- to detect or prevent crime, vandalism and public disorder in the town centres, particularly offences against the person
- to contribute to measures taken to reduce the incidence of crime, vandalism and public disorder in town centres
- to improve communication and the operational response of police patrols and the resources of partner agencies in and around the town centres including the command and control of major incidents

- to improve general security in the main retail streets, both in terms of personal security and security of buildings and premises, to contribute in making the town centres more attractive areas to shop and work in

- to monitor traffic flow

- to monitor major events such as carnivals and fairs which may take place within the towns

2.4 Excluding Offences and Certain Types of Behaviour

The system will not be used to prosecute minor traffic and parking violations.

2.5 Provision of Evidence

Recorded material resulting from the operation of the system will normally only be made available to the police for criminal investigation purposes. Recorded material are also made available to other enforcement agencies for criminal prosecutions in respect of the enforcement of bylaws, unlawful street trading and Health and Safety offences.

On occasion, specific requests are received from other organisations with prosecution powers such as H M Customs & Excise, the Health and Safety Executive and Trading Standards. In the event that evidence is required in connection with a prosecution which will assist in the achievement of the key objectives of the system, the evidence will be supplied if agreed by the data owner and controller and after consultation with the police. Any evidence supplied will be subject to an undertaking that it is only used in accordance with this Code of Practice and for the reasons for which it has been supplied.

2.6 Cameras

Consultation: the public space CCTV systems were installed following consultation between the former Cornwall Council, Devon & Cornwall Constabulary and the town councils and Chambers of Commerce of the towns where cameras are located.

Future Installation: Any future installation of CCTV cameras and ancillary equipment is considered in line with the advice and guidance contained in the Data Information Commissioner's CCTV Code of Practice – Version 1.2 and the Surveillance Camera Code of Practice Pursuant to Section 29 of the Protection of Freedoms Act 2012. It will be subject of documented consultation with interested parties, including the community.

Use of Sound: no sound is recorded by the system.

Change: before the introduction of any major technological change that will have a significant effect upon the capacity and/or operation of the system the implications is fully assessed in relation to the purpose and key objectives of the system and be the subject of public consultation. The introduction of other changes is fully assessed by the Partners and by agreement between them. The consideration and/or introduction of any change is reported in the Annual Report.

Dummy Cameras: public confidence in the system should be based on effective operating cameras and dummy cameras will not be used.

The areas to be covered by the system are public areas within the responsibility of the operating partners. So far as is possible all cameras will be placed in full public view. Cameras will not be deliberately hidden although circumstances may dictate that not all cameras will be visible from all areas of sight.

On occasion, mobile cameras may also be temporarily sited within an area. The use of such cameras, and the data produced by virtue of their use, will always accord with the objectives of the system and be governed by this Code of Practice and the procedures ancillary to it.

Signs: signs indicating that CCTV Cameras are operating are displayed at the perimeter of the areas covered by the system and at points within the town centres. The signs inform the public that cameras are in operation and allow people entering the area to make a reasonable approximation of the area covered by the scheme. The signs give an official contact telephone number. Cameras, whilst placed within public view, are not always individually indicated by placing a sign directly under each camera position. All siganage is check quarterly in line with the Town's maintenance agreement.

2.7 Monitoring and Recording Facilities

Each town in the system has a locally placed recording device, which records footage 24 hours a day, 7 days a week. From this location, a dedicated and secure line will link each town to the Cornwall Council Emergency Facility. A further dedicated and secure link will connect the Emergency Facility with the CFRCSS Critical Control Centre.

CCTV Operators at the CFRCSS Critical Control Centre are able to record images from selected cameras in real-time, produce copies of recorded images, replay or copy any recorded data in accordance with this Code of Practice. All viewing and recording equipment may only be operated by suitably trained and authorised users.

3. DATA PROTECTION

3.1 Registration under the Data Protection Act

The system operator is registered under the Data Protection Act 2018 in the name of Cornwall Council. The Partners and/or licensed Third Parties will take all necessary steps to comply with the detail and spirit of the Act and with each Partner's Data Protection Policy.

The Data Controller for the system is the individual town councils and day-to-day responsibility for managing the data is devolved to the Control Room Manager. All data is processed in accordance with the principles of the Data Protection Act 2018, which are, in summarised form:

- All personal data will be processed fairly and lawfully
- Personal data will be obtained only for the purposes specified

- Personal data held will be adequate, relevant and not excessive in relation to the purpose for which the data is processed

- Steps will be taken to ensure that data is accurate and, where necessary, kept up to date

- Personal data will be held for no longer than is necessary

- Individuals will be granted access to their personal data, in accordance with individual's rights

- Procedures will be implemented to prevent unauthorised or accidental access to, alteration, disclosure or loss and destruction of information

Information is not transferred outside the European Economic Area (EEA) unless the rights of individuals are protected.

3.2 Purpose for Which Data is Held

Data is held and stored only for the purpose set out in this Code of Practice and in accordance with its provisions.

3.3 Requests for Information (**Rights of Access, Rectification and Erasure Request)**

Any request from an individual for the disclosure of personal data which he / she believes is recorded by virtue of the System will be directed in the first instance to the Data Protection Officer in Cornwall Council.

The principles of the Data Protection Act 2018 shall be followed in respect of every request.

If the request cannot be complied with, without identifying another individual, permission from that individual must be obtained unless it is reasonable in all the circumstances to comply with the request without the consent of that individual.

Any person making a request must be able to satisfactorily prove their identity and provide sufficient information to enable the data to be located. The appropriate 'Closed Circuit Television (CCTV) **Rights of Access, Rectification and Erasure Request** form can be found on the Cornwall Council website or via this link https://www.cornwall.gov.uk/media/33315555/form-2018-rare-form-blank.pdf
We will not release images if doing so would impact upon a criminal investigation or infringe upon another person's privacy.

3.4 Exemptions to the Provision of Information

In considering a request made under the provisions of General Data Protection Regulations reference sections 6.1 and 9.2. General Data Protection Regulations includes, but is not limited to, personal data processed for any of the following purposes:

- The prevention or detection of crime
- The apprehension or prosecution of offenders

Data processed for these purposes is exempt from the subject access provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the matters referred to above.

4. CHANGES TO THE CODE

4.1 Review

The officers with overall responsibility identified in paragraph 1.5 ensure that this Code of Practice is reviewed and revised where appropriate every twelve months. Changes are introduced as necessary to ensure the efficient operation of the system.

4.2 Major Changes

A major change is one which will have a significant impact upon the Code of Practice or the operation of the system.

A major change will only take place after consultation with relevant interested groups and agreement between the Partners.

4.3 Minor Changes

A minor change is one which may be required for clarification and which will not have a significant impact upon the Code of Practice or the operation of the system. Minor changes are introduced by the partners as necessary and after such consultation as is considered appropriate.

4.4 Publication of Changes

All changes, whether major or minor, are reported in the system's Annual Report produced by Cornwall CCTV Management Group.

4.5 Operational Review

The partners, through their officers with responsibility for day-to-day management identified in para 6.1, will usually meet on at least a quarterly basis or as appropriate to review the operation of the system and of this Code of Practice.

Operational review will not always necessitate a meeting face to face but could take place in the form of e-mail correspondence or telephone conversation/s. The partners will constantly review the operation of the system and of this Code of Practice and proposals for improvement will be considered at these meetings or other discussions.

5. RESPONSIBILITIES OF THE OWNER OF THE SYSTEM

5.1 Principles

The Councils, as owners, have primary responsibility for compliance with the purpose and objectives of the system, for management and security of the system and the protection of the interests of the public and of the individual.

5.2 Implementation of the Code of Practice

The Councils, Police, Cornwall Fire and Rescue Service and Partners will ensure compliance with this Code of Practice.

Partners will ensure that adequate training is provided to operators and managers of the system and police officers using the system to ensure proper implementation of and compliance with this Code of Practice.

5.3 Accountability

The partners will comply with the requirements of this Code of Practice for accountability. The partners will provide information to the public about the operation of the system and about any proposed major changes to the system or this Code of Practice.

6. MANAGEMENT OF THE SYSTEM

6.1 Day-to-day Management

Day-to-day management of the system and the requirements of this Code of Practice for the partners are carried out by the manager of the CCTV Control room.

Day-to-day management of the staff engaged in the CCTV Control room is the responsibility of the manager of the centre, the appointed contractor or licensed third party dependant on local arrangements for resourcing monitoring services.

Day-to-day management on the part of Devon & Cornwall Constabulary will be with the Officer appointed.

These nominated officers shall meet on a quarterly basis, or otherwise shall liaise on a regular basis, over issues arising from the day-to-day operation of the system and if appropriate, shall raise issues with their senior officers for resolution by them.

6.2 Review

The officers (as identified in Section 1.5) with overall responsibility for the system on behalf of the Councils, Devon and Cornwall Constabulary, contractors and /or licensed third parties shall meet at least every six months or shall be consulted with via e-mail by the Responsible Officer as appropriate.
The purpose of the meeting is to review the operation of the system and the provisions of this Code of Practice.

6.3 Operational Procedures

Operational Procedures regulating the day-to-day operation of the Control room shall be produced and agreed between the partners and shall be drawn up in strict accordance with the principles of this Code of Practice.

The nominated officers responsible for day-to-day management of the system shall review the Operational Procedures as appropriate and shall revise them as necessary to ensure the efficient operation of the system. Changes to the Operational Procedures are only made if they are in accordance with the principles of this Code of Practice.

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

7. ACCOUNTABILITY

7.1 The Public

(a) Code of Practice and Complaints Procedure

This Code of Practice is a public document and hard copies will be available to view at the offices of the nine town councils and viewed on their respective websites. The Code of Practice is also published on the Cornwall Council website.

The formal complaints procedure of Cornwall Council is used for complaints about the system's use or operation, and this is also published on the Cornwall Council website.
https://www.cornwall.gov.uk/complaints

(b) Annual Reports

An Annual Report will be published which will be a public document available as in (a) above. The report will be for the year ending 31st March in any year.
The report will include:

- Reference to the number of incidents monitored and the action taken – where that information is available - made as a direct result of the system's use in relation to evidence gained

- The number and type of complaints made, information as required by this Code of Practice
- The details and outcomes of any review of camera locations with regard to Privacy Impact Assessments, necessity and proportionality
- Any other such information as is felt appropriate and useful to the public

7.2 The Councils

The Annual Report is presented to the councils and partners as soon as possible after its publication in each year.

7.3 The Police

The Devon & Cornwall Police will comply with this Code of Practice and give an account of doing so.

The Police are committed to operating and acting within this Code of Practice and the spirit of the objectives. They co-operate with the councils and the contractor in seeking to achieve these.

Where possible, the police provide information quarterly about the number of incidents, arrests, convictions, crime trends etc. to the council and this information, where available, will be included in the Annual Report.

8. PUBLIC INFORMATION

8.1 Principles

Despite the widespread use of public space CCTV, there may be public concern over the use of CCTV in public spaces. All partners involved in the system, work together to ensure that the privacy of individuals is not compromised. This is done in a number of ways including the completion of Privacy Impact Assessments, the use of strict controls on access to CCTV recordings and the monitoring room, and also controls over the location and coverage of the cameras.

The recording and retention of images of people in public places will be undertaken fairly and lawfully and information is not used for any purpose that has not been disclosed to the public in this Code of Practice or any subsequent Annual Report.

Members of the public should be aware that their image is being recorded. To this end, signage is erected as per paragraph 2.7 of this Code of Practice. This Code of Practice is also published on the websites of all partners.

9. ASSESSMENT OF THE SYSTEM AND CODE OF PRACTICE

9.1 Evaluation

Effective independent evaluation of the system is essential to identify whether the purposes of the system are being complied with and whether objectives are being achieved. Evaluation will either be conducted independently or carried out according to independently established criteria.

Evaluation of the system will include as a minimum:

- performance data
- operation of the Code of Practice
- whether the purposes for which the system was established still exist

The results of evaluations will be published as part of the Annual Report, as per paragraph 8.1 of this Code of Practice. The results of evaluations will be taken into account in the future functioning, management and operation of the system.

9.2 Monitoring

The person with day-to-day management of the system on the part of the councils will monitor the operation of the system and the implementation of this Code of Practice.

9.3 Audit

Regulatory bodies and/or auditors acting on behalf of Cornwall Council or other partners will regularly audit the operation of the system and this Code of practice.

The audit will include:

- compliance with this Code of Practice
- compliance with the Operational Procedures
- examination of Control room records, data histories and the content of recorded images

All partners will co-operate in the audits. Audit programmes will be agreed by the partners and findings and results will be shared between them.

9.4 Inspection

The councils shall introduce a system of independent inspection allowing the Inspectors access to records and to the Control room without notice.

Independent inspection will be carried out by individuals without any direct responsibility for the system and may include the appointment of an independent “lay visitor”.

10. STAFF

10.1 Principles

All staff – including volunteers - will be trained to Security Industry Association (SIA) standards and/or as is required by law. Well-trained and responsible staff or volunteers with good working conditions are essential for the proper and effective working of the system.

Staff employed or volunteers working in the control room, whether they be operators or managers should meet high standards of probity. Integrity and efficiency of staff or volunteers is achieved through effective recruitment, selection, training, vetting and management of staff or volunteers. Volunteers are only recruited through an accredited Volunteer Scheme or a recruitment process agreed between relevant partners.

All procedures concerning staff accord with employment practice incorporating equal opportunities standards.

Systems providing security and safeguards for recorded material and the system itself are the core of good management of the system.

In the event of standards laid down in the Code not being maintained disciplinary procedures will be implemented.

10.2 Recruitment and Selection

Any appointed contractor or other third party will adopt procedures which enable thorough checks upon the background of individuals to be carried out to ensure that candidates selected are suitable for work in a CCTV control room. This will include Non-Police Personnel Personal Vetting.

Non-disclosure of relevant matters by individuals will be the subject of disciplinary action and, if appropriate, dismissal.

10.3 Training

The partners ensure that all staff are trained to an appropriate level for the proper and effective working of the system. The Operational Procedures agreed by the partners are produced and constantly reviewed during the training process and throughout the undertaking of duties.

10.4 Confidentiality

All staff and volunteers will be subject to a requirement of confidentiality both during and after the termination of their employment.

11. COMPLAINTS

11.1 Principles

To obtain universal recognition, the interests of all who may be affected by the system will be recognised and the operation of the system will not be confined to the interests of the system owner or the needs of the Criminal Justice system.

11.2 Complaints Procedure

The complaints procedure of Cornwall Council is used in connection with the operation of the system and compliance with this Code of Practice within their respective areas. Details of the complaints procedure can be obtained from:

https://www.cornwall.gov.uk/complaints

or contacting the CCTV Control room via telephone 0300 1234 232.

These procedures are not intended to limit any other rights of complaint which the public may have, e.g. to the Data Protection Commissioner.

A record of all complaints received from third parties relating to the operation of the system and compliance with the Code of Practice will be kept by the Responsible Officer.

11.3 Police

Complaints about police action in connection with the system should be made in accordance with the statutory Police Complaints Procedure, which is available at any police station.

11.4 Annual Report

The Annual Report shall include information on the number of complaints received, of those complaints that have been substantiated and any action taken to remedy complaints.

Complaints which suggest a change of policy will be taken into account in any assessment of the system and the Code of Practice and will be kept by the Responsible Officer.

12. BREACHES OF THE CODE OF PRACTICE INCLUDING THOSE OF SECURITY

12.1 Responsibility

Principal responsibility for the system rests with the Cornwall Fire, Rescue and Community Safety Service using the Policy and Procedures of Cornwall Council. They will ensure that all breaches of this Code of Practice and of security are investigated and remedied.

Where a serious breach has occurred, the councils will appoint a person with relevant professional qualifications, independent from the operation of the system, to investigate the breach and make recommendations on how the breach may be remedied.

All partners, contractors and third parties will co-operate in the investigation of any breaches which may occur, the consideration of investigation reports and the implementation of any measures considered appropriate as a result of the investigation.

13. CONTROL AND OPERATION OF CAMERAS

13.1 Principles

Information recorded should be accurate, adequate, relevant and should not exceed that necessary to fulfil the purposes of the system.

Information recorded should be obtained fairly and in accordance with the provisions of this Code of Practice on privacy.

13.2 Camera Operation

The operators of camera equipment shall act with the utmost propriety at all times.

Only those staff with direct responsibility for using the equipment shall have access to the operating controls.

All use of the cameras shall accord with the purposes and key objectives of the system and shall comply with this Code of Practice.

Cameras shall not be used to look into private property. Where appropriate, operational procedures and technological measures will be adopted to impose restraints upon the use of cameras in connection with private premises.

Camera operators shall at all times be subject to supervision sufficient to ensure compliance with this part of the Code of Practice.

All camera operators and supervisors shall be made aware that all recordings are subject to routine audit and that they may be required to justify their interest in a member of the public or premises.

The effectiveness of individual operators shall be subject to regular review and contractors or third parties shall ensure that its operators act at all times in accordance with current best practice.

13.3 Primary Control of the Cameras

Primary control of the cameras is held by Cornwall Fire, Rescue and Community Safety Service. If access to images is permitted elsewhere, such as in some towns and police facilities, operations must fully adhere to all principles and guidance in this Code of Practice and associated documentation.

14. ACCESS TO AND SECURITY OF MONITORS AND CRITICAL CONTROL CENTRE

14.1 Principles

Only those with a legitimate reason to do so shall have access to the control room.

Only those with a legitimate reason to do so, and being appropriately trained and SIA-qualified, shall operate or view the equipment and its outputs, whether recordings or photographs.

Regard is made to the provisions of this Code of Practice on privacy.

14.2 Monitors

Access to view monitors, whether to operate the equipment or to view the images, is restricted to staff with access rights to the control centre.

A Control room Occurrence Record shall record staff on duty each shift and the names of any persons or groups that have been authorised by the person with day-to-day management of the system for the Councils to have access to the Control room and/or view the monitors.

A responsible operator will be present during the operation of monitors. If monitors are to be left unattended the room in which they are kept will be secured against unauthorised entry.

Public access to or the demonstration of monitors shall not be allowed except for lawful, proper and sufficient reasons. The need to ensure security and privacy of individuals is paramount in this respect.

14.3 Control Room

Arrangements for the control room include requirements to ensure that the control room is secure at all times. These are set out in the Operational Procedures and include:

- Routines and procedures and any other facilities necessary to ensure that the control room is protected from unauthorised access

- All supervised individuals entering the control room, such as CCTV contractors are supervised by control room staff. They must comply with this Code of Practice and associated legislation and protocols including the restrictions relating to the information seen or heard in the control room during the course of their business

- Unsupervised access to the control room is limited to those personnel who are appropriately SIA trained. The control room is staffed 24 hours a day, 7 days a week, and access is achieved through validated ID cards, which are only held by trained control room staff

- Records shall be kept of all access to the Control room recording details of the individual concerned and time of arrival and departure

- Operation times and the numbers of staff on shift shall be clearly defined and complied with

- Access to the Control room shall be restricted to staff with access rights

- Technical repairs, cleaning and similar tasks shall be carried out in controlled circumstances

- Access by visitors shall be carefully defined and shall be the responsibility of the Cornwall Fire, Rescue and Community Safety Service

- Police visits (save for those made by police officers with image reviewing responsibilities) shall be pre-arranged – where the Control room is staffed - and made in order to view, collect or return recorded images. Any other visits by police must either comply with other provisions of this Code of Practice or the purpose of the visit shall be established, confirmed and approved by the Control Room Manager.

- Auditors and independent inspectors appointed under the Code of Practice may visit without prior appointment (see Section 10).

14.4 Supervision and Audit

Security procedures on access to the control room shall be maintained and strictly honoured. Access shall be monitored and all concerned must know that security procedures on access to the control room are included in the regular audit.

14.5 Occurrence Record

An Occurrence Record or Log shall be maintained on the basis of time and date/day throughout operations and brief details given of all occurrences within the control room, including particulars of visits and of telephone calls.

14.6 Health and Safety

Compliance with Health and Safety legislation is a requirement of this Code of Practice.

15. RECORDED MATERIAL

15.1 Principles

For the purposes of this code, 'recorded material' refers to any material recorded by, or capable of being produced as a result of, technical equipment which forms part of the system. This specifically includes images recorded digitally, including still images.

Recorded material may be admitted in evidence. It must be of good quality and be accurate in content. Recorded material must be treated according to defined procedures to provide continuity of evidence and to avoid contamination of the evidence.

Appropriate security measures shall be taken against unauthorised access to, alteration, disclosure, destruction or accidental loss of recorded material.

Recorded material is held only for the purposes provided by this Code of Practice.

Information recorded is accurate, adequate, relevant and not exceed that necessary to fulfil the purposes and key objectives of this system.

Recorded material is kept no longer than is necessary for the purposes and key objectives of the system. It is then be safely destroyed.

Members of the public may be confident that information recorded about their ordinary activities in the area covered by the cameras is treated with regard to their individual privacy.

Recorded material will not be copied, sold, or otherwise released or used for the provision of entertainment or otherwise made available for any use incompatible with this Code of Practice.

15.2 Statement of Intent

In accordance with the principles underlying this section the Councils adopt the following Statement of Intent on the use of and access to recorded material:

(a) recorded material shall be used only for purposes defined in this Code of Practice

(b) access to recorded material shall only take place as defined in this Code of Practice

(c) recorded material shall not be sold or used for commercial purposes or the provision of entertainment

(d) the showing of recorded material to the public shall only be allowed in accordance with the law; either in compliance with the needs of the police in connection with the investigation of crime which will be conducted in accordance with the provisions of any relevant Code of Practice under The Police and Criminal Evidence Act 1984, The Criminal Procedure and Investigations Act 1996 and any advice and guidance given to the Police from time to time; or in other circumstances provided by the law.

15.3 Ownership

Ownership of recorded material and copyright in recorded material is that of the town councils as owner or operator of the system.

15.4 Recording Equipment

Recording equipment shall be checked at least weekly to ensure it is in good working order.

15.5 Use of DVDs (the term DVD shall also apply to CDs)

A supply of DVDs shall be maintained which is sufficient for the purpose of downloading images of evidential value.

All DVDs shall be of a type manufactured or encrypted to prevent overwriting of downloaded material.

Recorded material is kept on physical storage media for 120 days from the date of burning, in a secure store within the CCTV suite. An audit of media and associated paperwork is done monthly and media over 120 days will be destroyed in accordance with the destruction of data policy.

When images are downloaded to a DVD, that DVD will become the Master Copy and the responsibility of the police, once signed over to them.

The original image retention policy shall be made known to the police, the Crown Prosecution Service and the local Law Society.

15.6 Cataloguing, Storage and Recording of DVDs (Use of digital storage includes in 15.12)

DVDs used to record images providing evidence shall be individually and uniquely identified.

A Register shall be maintained detailing when images are downloaded and by whom.

The Register shall be secure.

15.7 Evidential Use of Recordings

DVDs required for evidential purposes are treated as exhibits.

Any DVD that is provided for evidential purposes must be of proven integrity.

Where applicable non-police staff will provide the police with statements required for evidential purposes.

15.8 Police Access to Recorded Data

Police may apply for access to recorded material, in accordance with this code, where they reasonably believe that access to specific images is necessary for the investigation and detection of a particular offence or offences or the prevention of crime.

The police will apply for access via an Authority To View (ATV) form, countersigned by a supervisory police officer, who will occupies the rank of Sergeant or above. A copy of the form is found at Appendix C.

In urgent cases, for example where an arrest has been made, the CCTV control room will provide a disc of evidence to the police upon request, upon receipt of an ATV form.

The CCTV control room will provide a “review” service to the police upon request, via ATV form. In non-urgent cases, staff in the control room will endeavour to review requested footage within seven days and provide either a negative return, a disc showing evidence, or a disc for court disclosure, to the police.

Live images may from time to be time be displayed in the Multi-Agency Silver Control Room (Emergency Centre), for example during major incidents (such as flooding, serious fires, explosions

or firearms incidents) or during major events (such as Royal Visits or large community events where the Silver room is opened).

Access to the Silver Room is restricted by Cornwall Council access pass and only staff who are required to be present for the management of the specific incident will be permitted access to the room. This may include other emergency or statutory agencies necessary to manage the incident, such as the Environment Agency (in cases of flooding for example) or the Ambulance Service (in cases involving mass causalities). No CCTV images will be removed from the room without appropriate authority (completed ATV form).

Live images may be displayed within the police control room. Access to this room is strictly controlled and restricted to the control room staff who are required to operate the control room and escorted visitors only. No CCTV images will be removed from the room without appropriate authority (completed ATV form).

Members of the police service or other agency having a statutory authority to investigate and/or prosecute may release details of recorded information to the media only in an effort to identify alleged offenders or potential witnesses. Police may also show material to witnesses for the purposes of obtaining identification evidence. Under such circumstances, full details are recorded in accordance with the Operational Manual, by the holder of the data.

The protocol for access to data at police stations can be found at Appendix D.

15.9 Access to Recorded Images by Data Subjects

Under the Data Protection Act 2018 a Data Subject (i.e. the individual who is the subject of the personal data) has the right to access recorded images of themselves. This access will be facilitated using the Data Protection principles of Cornwall Council.

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

- the request is made in writing
- the data controller is supplied with sufficient information to satisfy him or herself as to the identity of the person making the request
- 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 is unlikely to know the precise time. Under those circumstances it is suggested that within one hour of accuracy would be a reasonable requirement)
- the person making the request is only shown information relevant to that particular search and which contains personal data of her or himself only, unless all other individuals who may be identified from the same information have consented to the disclosure

In the event of the data controller complying with a request to supply a copy of the data to the subject, only data pertaining to the individual should be copied, (all other personal data which may facilitate the identification of any other person should be concealed or erased). Under these circumstances an additional fee may be payable.

The data controller is entitled to refuse an individual request to view data under these provisions if insufficient or inaccurate information is provided, however every effort should be made to comply with subject access procedures and each request should be treated on its own merit.

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

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

15.10 Primary Request for Access to and Disclosure of Images to Third Parties

Access to and disclosure of images to third parties will be restricted to:

- law enforcement agencies where the images recorded would assist in a specific criminal enquiry
- prosecution agencies
- legal representatives
- the news media, where it is assessed by the police that the assistance of the public is needed in the identification of a victim, witness, vehicle or perpetrator in relation to a criminal incident or to minimise risk to a person(s) deemed vulnerable. As part of that assessment, the wishes of the victim of an incident or relatives of a vulnerable person must be taken into account. Where data is to be released in such a way, the police will assume responsibility for the release of this, and will do so by requesting the images in the usual way, using an appropriately authorised ATV form
- the people whose images have been recorded and retained (unless disclosure to an individual would prejudice the criminal enquiries or proceedings)
- staff during the course of their training and education

Any such disclosure will be in accordance with the Data Protection Act 2018 and this Code of Practice. Access and disclosure is facilitated using the Data Protection procedures of Cornwall Council.

15.11 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:

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

- in respect of material to be released under the auspices of 'crime prevention', written agreement to the release of the material should be obtained from a police officer, not below the rank of Inspector. The officer should have personal knowledge of the circumstances of the crime/s to be prevented and an understanding of the CCTV System Code of Practice (2).
- if the material is to be released under the auspices of 'public wellbeing, 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 System Code of Practice.

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

15.12 Use of cloud based services for data transfer

Cornwall Fire and Rescue, part of Cornwall Council, have adopted Microsoft Office 365 Sharepoint as a method for transferring CCTV data to prosecuting agencies.

- **Security** Cornwall Council are in contract with Microsoft and manage a secure tenant to host

services used by Cornwall Council. This tenant uses secure web protocols and encryption to ensure information is kept safe. All information is held in secure data centres within the EU or UK.

- **Access to information** User access is maintained by CFRCSS Critical Control Centre. Access to upload is only available to licenced CCTV operators. Access to download footage is only available to nominated accounts from prosecuting agencies. Access is setup to deny access to information not relevant to that user account.
- **Risk Assessment** CFRCSS have undergone a comprehensive internal Business Privacy Impact Assessment. This has been signed off by the Cornwall Council Data Protection Team.
- **Retention of data** Recorded material is kept on cloud storage for 120 days from the date of burning. Media over 120 days will be purged by an internal automated process, setup on the cloud service.

16. PHOTOGRAPHS

16.1 Still Photographs

Still photographs are not taken as a matter of routine. The taking of each photograph must be capable of justification, with the originator of the photograph being responsible for ensuring that its capture and use complies with current regulations and is managed in accordance with the Operational Manual and this Code of Practice.

16.2 Taking Still Photographs during Live Incidents

Still photographs from live incidents are only be taken at the request of the police officer in charge at the scene when that officer shall be identified, and a record made of the request together with details of the incident and time and date of the request.

16.3 Production of Stills

A police officer authorised by a police officer of at least the rank of Sergeant may request that an operator produce a still photograph taken at a live incident, or still photographs from recordings. The authorising police officer shall be satisfied that the still photograph is required for the prevention or detection of crime.

16.4 General

All still photographs shall remain the property of the System Operator and shall be indexed in sequence. A record is kept of the reason for production of the photograph, the identity of the person requesting it, date and time, the particulars of production of a live photograph and information identifying the control room staff member responsible for producing the photograph.

Any still photograph released to the police shall be dealt with by the police as an exhibit and shall, at no time, be used for anything other than the purpose specified and identified when released to the police.

All still photographs are destroyed within 28 days unless made the subject of an application from the police or are required as evidence. A record is kept of the destruction of all photographs.

The use of photographs for briefing camera operators is conducted strictly in accordance with advice from the police to avoid contamination of evidence. Unless otherwise advised by the police, photographs:

- shall not be on display and shall be kept in a binder or album, with the exception only of still photographs which are displayed on any of the display boards in the control room. These display boards must be covered before anyone other than staff or police enter the control room

Procedures under this part of this Code of Practice may be the subject of monitoring and audit. A police officer, appointed in accordance with the liaison arrangements in this Code of Practice, shall be allowed access from time to time to check compliance with these requirements.

17. DEALING WITH INCIDENTS

17.1 Principles

Incidents are dealt with according to Operational Procedures agreed by the partners and the provisions of this Code of Practice.

17.2 Procedure for Dealing with Incidents

The notification of incidents shall be a two-way flow of information between the police and the system operators

When a camera operator sees a suspicious incident, the operator shall notify the Police Operations Room, log the incident on the Incident Register and log this in the Operators' Handbook.

On receiving the information, the Police Operations Room staff will assess the situation, create a log, and decide the action to be taken. This may include the deployment of a resource to respond to the incident, a request for continual monitoring of the incident, a request for camera pictures to be displayed at the Operations Room or a particular police station (where technically available);

All incidents reported to the police shall be logged in the control room Incident Book/Secure Database including the time and date of incident; Log No; town incident occurred within; camera and console details used for recording of the incident; details of incident; signature of monitoring operator.

17.3 System Control

The control of the CCTV system rests with the manager of the CCTV Control room.

Cameras may also be controlled at the local police stations or town centre control rooms (where technically available and subject to paragraph 14.3 of this Code of Practice). Police control of cameras will only occur when properly authorised.

Real time recording of camera images is carried out on secure equipment installed in each town.

Review of recorded images can take place in the control room or at selected secure police stations. All viewing of recorded images carried out at police stations will comply with paragraph 16 of this Code of Practice.

18. POLICE CONTACTS AND USE OF THE STATION

18.1 Principles

Relations between control room staff, representatives of the town councils and the police are conducted strictly in compliance with this Code of Practice. These requirements are not exceeded informally and the different roles and responsibilities of staff and police are acknowledged and respected.

18.2 Routine Contact

Officers shall be identified by the police and any contractors or licensed third parties for liaison for day-to-day purposes. Senior staff are nominated for liaison on audit and for decisions with significance for the operation and management of the system.

Access to recorded images and to the control room comply with this Code of Practice and the time and date and purpose of such access is recorded and monitored.

Where it is technically possible to control cameras or view camera images other than in the control room, such control or viewing must accord with this Code of Practice and Operational Procedures.

In relation to telephone calls received from the police a note is entered in the Operator's personal console notebook as appropriate.

18.3 Police Use of the System

Police use of the system in any manner must accord with this Code of Practice and protocols developed between the town councils and the police. Such protocols are grounded in this Code of Practice and do not extend beyond it nor exclude any aspects of it.

Use of or takeover of control of the system shall be in clearly defined circumstances agreed according to local needs and the purposes of the system, be revised annually in the context of the local policing plan and be according to this Code of Practice.

Should a request from the police for use of the system in any manner arise, that is not provided for by this Code of Practice, it shall be the subject of a specific agreement between the CCTVMG, members as specified in paragraph 1.5 of this Code of Practice, and the police.

Any use of the system is recorded in the Control Room Occurrence Record and by the police and be subject to audit by both council and police procedures. In the control room, reasons for use shall be required and recorded in the Occurrence Book with particulars of date and time and the name of the officer making the request. Records are retained by police recording the same particulars and the officer taking responsibility for the decision.

19. AIRWAVES RADIOS – USE AND SECURITY

19.1 Principles

Airwave is a National Radio Scheme for the British Fire Service (excluding Northern Ireland). The system uses trunked digital technology allows much clearer voice messages than the existing analogue system. The system allows data transmissions. The other major benefit of system is it will allow interoperability between each Fire, Rescue and Community Safety Service and with the police and ambulance services.

The Airwave radio scheme is used by the police and other agencies and there is a high level of security imposed by Government on the system. Due to the radio scheme being digital, it is only possible to monitor radio traffic using an Airwave radio.

Author: Sarah Kind
Organisation: Cornwall Fire, Rescue and Community Safety Service
Contact: Sarah Kind
E mail: skind@fire.cornwall.gov.uk

Appendix A: CCTV Camera Locations

Penzance	St Ives	Hayle	Camborne
Clarence Street HSBC Market Place Causeway Head Middle Causeway Head Top Market Place (Burtons) Chapel Street Star Inn Market Jew Street x2 Wharf Road Car Park Clarence St Car Park Bus Station Car Park Jubilee Pool Alexandra Park Princess May Rec Grd Bus Station Toilets Princess May Rec Grd (Toilets)	The Terrace Tregenna Co-Op Mountain Warehouse Wharf Road Malakoff	Co-Op Cornubia Inn Library Spar Shop Skate Park Philps Pasty Shop	Whetherspoons Argos Rowes Pasty Cross Street Fish and Chip Shop Wesley Street Barclays Bank

Redruth	Helston	Falmouth	Penryn
Old Police Station Fore Street West End Fore Street (Premier) New Cut Car Park Alma Place West End Viaduct	Lloyds Bank Market Street Church Street Meneage St (Oxfam) Meneage St Coinagehall Street Co-Op Car Park Bowling Green Ope Way Sunken Garden	Watersports Centre Trago Mills Custom House Quay Cribbs Church Corner Anns Cottage Church St Car Park Grapes Inn M&S Superdrug Prince of Wales Pier Lower High Street Toni & Guy Dominos The Moor (Taxi Rank) Quarry Hill Car Park Grove Place Car Park Brook Place	Broad Street Lloyds Pharmacy Post Office

Truro	Perranporth	Wadebridge	Bodmin
Quay Street	St Georges Hill	Camel Trail (Padstow)	Skate Park
River Street	Boscawen Road	The Platt	Football Pitch
Victoria Square	Beach Road	Bridge East	Car Park
St Nicholas Street	St Pirans Road	Car Park	St Nicholas Street
Cathedral Lane	Station Road	Pavillions	Mount Folly
Boscawen Street	Skate Park	Camel Trail (Bodmin)	Clock Tower Folly
Lemon Quay	Cliff Road		Turf Street
Bus Station	Waterfront		Fore Street
Halfords			Whetherspoons
New Bridge Street			Higher Bore Street
St Marys Street			Clock Tower
Wilkes Walk			Fair View Park
Moorfield Car Park			Priory Road
Walkers Car Park			
Pydar Street (Bottom)			
Pydar Street (Top)			
The Leats			
Calenick Street			
St Georges Road Skate Park x 2			
Mallets			

Liskeard			
Barras Place			
Pike Street			
Baytree Hill x2			
Roundabout			
Cattle Market			
Cattle Market Car Park			
Lux Street			

Appendix B: Cornwall CCTV Management Group Partners (HARD COPY HELD ON FILE)

We, as Partners involved in the provision, use and operation of the Cornwall CCTV System commit ourselves to act only in accordance with the applicable law, this Code of Practice and the Cornwall Public Space CCTV Operational Procedures Manual.

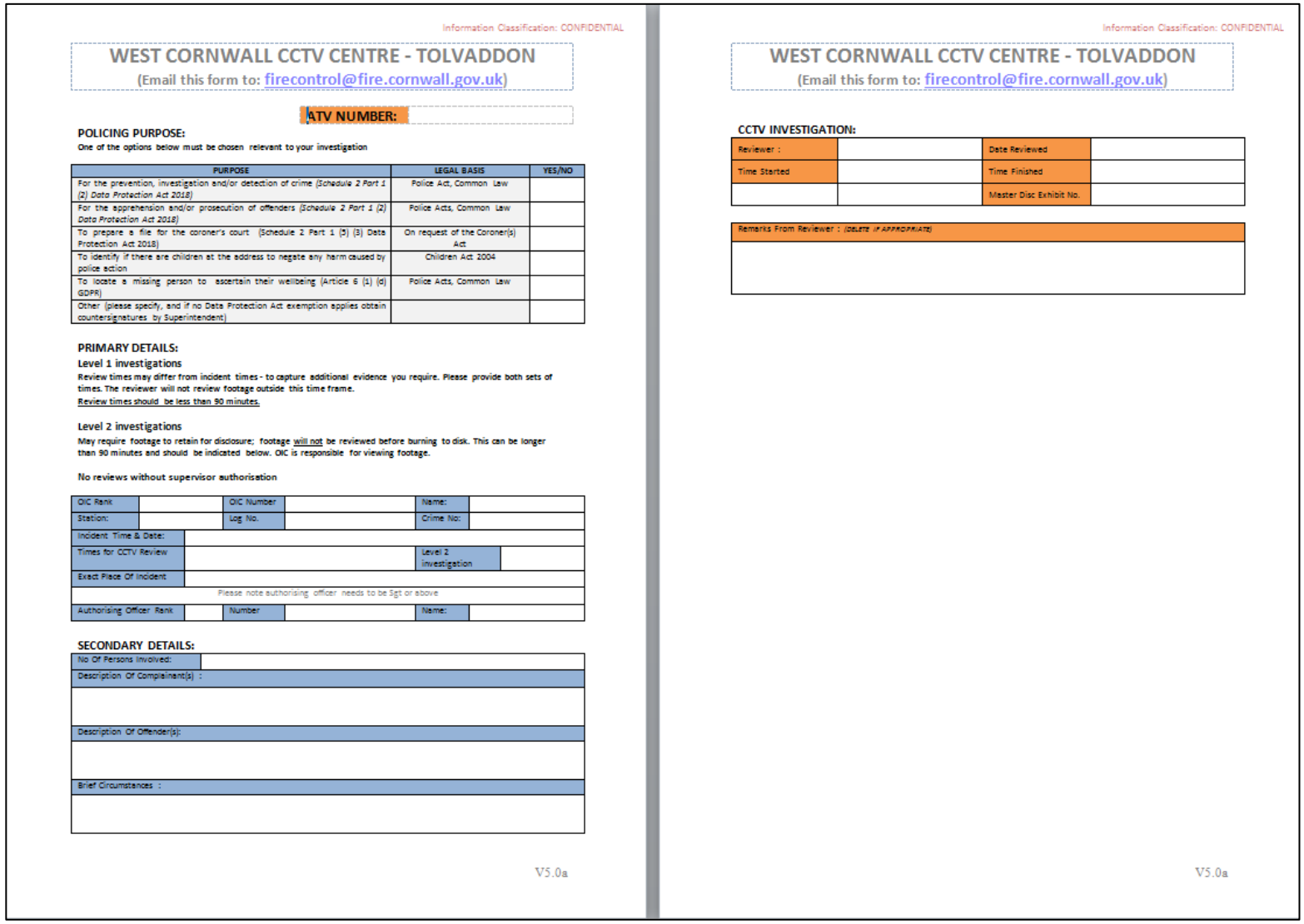
Penzance	St Ives	Hayle	Camborne
Signed: Name: Role: Date:	Signed: Name: Role: Date:	Signed: Name: Role: Date:	Signed: Name: Role: Date:

Redruth	Helston	Falmouth	Penryn
Signed: Name: Role: Date:	Signed: Name: Role: Date:	Signed: Name: Role: Date:	Signed: Name: Role: Date:

Truro	Perranporth	Wadebridge	Bodmin
Signed: Name: Role: Date:	Signed: Name: Role: Date:	Signed: Name: Role: Date:	Signed: Name: Role: Date:

Liskeard		Police represenative	
Signed: Name: Role: Date:		Signed: Name: Role: Date:	

Appendix C: Authority to View (V5a)



Information Classification: CONFIDENTIAL

WEST CORNWALL CCTV CENTRE - TOLVADDON

(Email this form to: firecontrol@fire.cornwall.gov.uk)

ATV NUMBER:

POLICING PURPOSE:

One of the options below must be chosen relevant to your investigation

PURPOSE	LEGAL BASIS	YES/NO
For the prevention, investigation and/or detection of crime *(Schedule 2 Part 1 (2) Data Protection Act 2018)*	Police Act, Common Law	
For the apprehension and/or prosecution of offenders *(Schedule 2 Part 1 (2) Data Protection Act 2018)*	Police Acts, Common Law	
To prepare a file for the coroner's court (Schedule 2 Part 1 (5) (3) Data Protection Act 2018)	On request of the Coroner(s) Act	
To identify if there are children at the address to negate any harm caused by police action	Children Act 2004	
To locate a missing person to ascertain their wellbeing (Article 6 (1) (d) GDPR)	Police Acts, Common Law	
Other (please specify, and if no Data Protection Act exemption applies obtain countersignatures by Superintendent)		

PRIMARY DETAILS:

Level 1 investigations

Review times may differ from incident times - to capture additional evidence you require. Please provide both sets of times. The reviewer will not review footage outside this time frame.

Review times should be less than 90 minutes.

Level 2 investigations

May require footage to retain for disclosure; footage will not be reviewed before burning to disk. This can be longer than 90 minutes and should be indicated below. OIC is responsible for viewing footage.

No reviews without supervisor authorisation

OIC Rank		OIC Number		Name:	
Station:		Log No.		Crime No:	
Incident Time & Date:					
Times for CCTV Review				Level 2 investigation	
Exact Place Of Incident					
Please note authorising officer needs to be Sgt or above					
Authorising Officer Rank		Number		Name:	

SECONDARY DETAILS:

No Of Persons Involved:
Description Of Complainant(s) :
Description Of Offender(s):
Brief Circumstances :

V5.0a

Information Classification: CONFIDENTIAL

WEST CORNWALL CCTV CENTRE - TOLVADDON

(Email this form to: firecontrol@fire.cornwall.gov.uk)

CCTV INVESTIGATION:

Reviewer :		Date Reviewed	
Time Started		Time Finished	
		Master Disc Exhibit No.	

Remarks From Reviewer : *(DELETE IF APPROPRIATE)*

V5.0a

Appendix D: Monitoring and Reviewing Equipment at Police Stations

There are two scenarios in which police personnel may view CCTV images: for general monitoring purposes, such as a large gathering of people, or targeted surveillance. In either scenario, police may view live images or playback, but all requests for downloading images must be directed to the control room, which will produce DVDs of footage in the normal way, with an ATV form.

General Monitoring of Large Gatherings (Viewing Only)

Where there is a terminal at a police station or police headquarters, which is only capable of receiving images and not reviewing or downloading, there will be no specific restriction on access to these images as the existing secure access to the building is proportionate and reasonable to ensure no excessive or inappropriate viewing takes place. Viewing images in this manner shall be restricted to general surveillance, such as monitoring a large gathering of people.

The images remain under direct control of the Control Room. The Control Room will maintain a register of all such requests, which will detail

- Officer requesting
- Reason for request
- Date & Time and duration of viewing
- The requesting officer will be responsible for the communication with the control room, which will maintain control of the cameras

Reviewing

Where there is a terminal at a police station/ police headquarters which is capable of receiving images and also of reviewing footage, the following policy applies:

- Only Officers / Staff who are specifically trained and authorised to use the terminal will do so
- Details of such authorised officers will be provided to the Control Room
- There will be a maximum of 12 officers authorised for each terminal
- Each authorised officer will have specific training on use of the software, and refresher input on the legal parameters for use of data
- Each officer will have a unique personal password so that each and every access and action can be audited if necessary
- Footage of a potentially evidential nature will only be downloaded by control room staff, following the submission of an ATV form, in the usual manner

Targetted Surveillance

When a camera is used for targeted surveillance, the correct authorisations under RIPA (Regulation of Investigatory Powers 2000) will be required. Surveillance undertaken in this way will be covert, that is, without the knowledge of the person who is the subject being monitored. In addition, this type of

surveillance may be intrusive, that is, taking place on any residential premises or inside a vehicle or of such a high quality that the camera may have been inside those premises or vehicle.

Directed surveillance is defined as covert surveillance that has been undertaken in relation to a specific investigation, which is likely to obtain private information about a person in a public place. Examples of this type of surveillance may include the tracking of a named individual whilst they are located within the CCTV operating zone.

RIPA authority is not required to observe a hot spot area, such as a known area for drug dealing, as the monitoring is not targetted at an individual.

Where the police wish to make use of CCTV monitoring in a pre-planned, covert and/or directed manner, authorisation must be given by an officer of Police Superintendant rank or above. In some situations, authorisation may be required immediately, in which case an Inspector or above may provide this, although this authorisation would only be valid for a period of 72 hours. In either case, the grounds for authorisation are:

- National security
- Prevention and detection of crime
- Preventing disorder
- Protecting public health
- In the interests of public safety

Where possible, CFR&CSS will inform the town council of a RIPA request, when it is received. Where the situation is of an urgency that will prevent this, CRF&CSS will action the request in accordance with the Code of Practice, but must inform the town council as soon as possible after the fact.