

Rhondda Cynon Taf County Borough Council Public Space Surveillance CCTV Scheme



Policy Document 2021

Code of practice for the management and operation of the Public Space CCTV System

Complying With:

BS 7958:2015 Closed Circuit Television (CCTV) – Management and Operation - Code of Practice

BS 7499: 2013 Static Site Guarding and Mobile Patrol Services – Code of Practice (Relevant Parts)

BS 7858: 2012 Security Screening of Individuals Employed in a Security Environment – Code of Practice

Information Commissionaire CCTV Code of Practice

Home Office Surveillance Camera Code of Practice

Contents

Section

1. Introduction and Objectives (Page 3)
2. Statement of Purpose (Page 4)
3. Principles and Policies (Page 7)
4. Accountability and Public Information (Page 12)
5. Assessment of the system and Code of Practice (Page 13)
6. Control and Operation of Cameras (Page 14)
7. Access and security for the Control Centre and associated equipment (Page 18)
8. Management of recorded material (Page 19)
 - Appendix A Key Personnel
 - Appendix B RCT CCTV Sign
 - Appendix C Restricted Access Notice
 - Appendix D Camera locations

1.0 INTRODUCTION AND OBJECTIVES

Introduction

A Closed Circuit Television (CCTV) system has been introduced to Rhondda-Cynon-Taf CBC. This system, known as the 'Rhondda-Cynon-Taf CBC Town Centre CCTV System (hereinafter known as the System)', comprises a number of cameras installed at strategic locations. All are fully operational with pan, tilt and zoom facilities. Others are fixed cameras, images from which are presented in the same room. For the purposes of this document, the 'owner' of the system is Rhondda Cynon Taf CBC. For the purposes of the Data Protection Act the 'data controller' for the system is the CCTV Senior Officer. The 'system manager' is the CCTV Senior Officer. The System has been notified to the information Commissioner. Details of key personnel, their responsibilities and contact points are shown at Appendix A to this Code.

Partnership statement in respect of The Human Rights Act 1998

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, and consider that the use of CCTV in Rhondda Cynon Taf is a necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve public safety.

This assessment is evidenced by an agreed 'operational requirement' document. 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 and it is also considered a necessary initiative by the Partners towards their duty under the Crime and Disorder Act 1998.

It is recognised that operation of The System may be considered to infringe on the privacy of individuals. The Partnership recognise 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 in so far as it is necessary in a democratic society, in the interests of national security, public safety, the economic well being of the area, for the prevention and detection of crime or disorder, for the protection of health and morals, or for 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 to ensure there is absolute respect for everyone's right to a free trial.

The System 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.

Objectives of the System

The objectives of The System as determined by the owners/partners which form the lawful basis for the processing of data are:-

- *To help reduce the fear of crime*
- *The help deter crime*
- *To help detect crime and provide evidential material for court proceedings*
- *To assist in the overall management of the Town Centres in Rhondda Cynon Taf covered by its town centre CCTV system*
- *To enhance community safety, assist in developing the economic well being of the area and encourage greater use of the Town Centres, shopping areas car parks etc*
- *To assist the Local Authority in its enforcement and regulatory functions within the areas covered*
- *To assist in supporting civil proceedings which will help detect crime*
- *To assist in the training of CCTV operator, the Police and others involved in the use of the CCTV system*

Procedural Manual

This Code of Practice (hereafter referred to as ‘the Code’) is supplemented by a separate ‘Procedural Manual’ which offers instructions on all aspects of the day-to-day operation of the system. To ensure the purpose and principles of the CCTV system are realised, the procedural manual is based and expands upon the contents of this Code of Practice.

2.0 Statement of Purpose

Purpose

The purpose of this document is to state the intention of the owners and the managers, on behalf of the partnership as a whole and as far as is reasonably practicable, to support the objectives of *The System* and to outline how it is intended to do so.

The ‘Purpose’ of the system, and the process adopted in determining the ‘Reasons’ for implementing ‘The System’ are as previously defined in order to achieve the objectives detailed within Section 1.

General Principles of Operation

The system will be operated in accordance with all the requirements and the principles of the Human Rights Act 1998.

The operation of the system will also recognise the need for formal authorisation of any covert 'Directed' surveillance or crime -trend (hotspot') surveillance as required by the Regulation of Investigatory Powers Act 2000 and the police force policy.

The system will be operated in accordance with the Data Protection Act at all times

The System will be 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 will be operated with due regard to the principle that everyone has the right to respect for his or her private and family life and their home.

The public interest in the operation of the system will be recognised 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.

Copyright

Copyright and ownership of all material recorded by virtue of The System will remain with the data controller.

Cameras and Area Coverage

Cameras offer full colour, pan tilt and zoom (PTZ) capability, some of which may automatically switch to monochrome in low light conditions.

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

Monitoring and Recording Facilities

A staffed monitoring room is located at a suitable location within RCT. The CCTV equipment has the capability of recording all cameras simultaneously throughout every 24 hour period

Secondary monitoring equipment may be located in (other) [police] premises. No equipment, other than that housed within the main CCTV control room shall be capable of recording images from any of the cameras.

CCTV operators are responsible for recording images from selected cameras in real-time, and assist in producing recorded images, replay or copy any pre-recorded data at their discretion and in accordance with the Code of Practice. All viewing and recording equipment shall only be operated by trained and authorised users.

Human Resources

Unauthorised persons will not have access without an authorised member of staff being present.

The monitoring room shall be staffed by specially selected and trained operators in accordance with the strategy contained within the procedural manual.

All operators shall receive training relevant to their role in the requirements of the Human Rights Act 1998, Data Protection Act 2018 and GDPR2016, Regulation of Investigatory Powers Act 2000 and the Codes of Practice and Procedures. Further training will be provided as necessary.

Processing and Handling of Recorded Material

All recorded material, will be processed and handled strictly in accordance with this Code of Practice and the Procedural Manual.

Operators Instructions

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

Changes to the Code or the Procedural Manual

Any major changes to either the Code of Practice or the Procedural Manual, (i.e. such as will have a significant impact upon the Code of Practice or upon the operation of the system) will take place only after consultation with, and upon the agreement of all organisations with a participatory role in the operation of the system.

A minor change, (i.e. such as may be required for clarification and will not have such a significant impact) may be agreed between the manager and the owners of the system.

Notes

- I. The installation of a CCTV camera is considered to **be overt** unless it is installed in a manner whereby its presence is deliberately intended to be concealed from the view of any person likely to be within the field of view of that camera.
- II. Cameras which may be placed in domes or covered to reduce the likelihood of assessing their field of view, or to protect them from weather or damage, would not be regarded as covert provided that appropriate signs indicating the use of such cameras are displayed in the vicinity.
- III. The use of 'dummy' cameras as part of a CCTV System is strongly discouraged. The greatest deterrent value of a CCTV System is its power to produce evidential material and, in doing so, to reassure those it is intended to protect.
- IV. It is acknowledged that many CCTV Systems are operated on a 'part time' basis or without the benefit of a staffed monitoring room. In such cases reference to 'monitoring rooms' throughout this Code should be applied to existing monitoring and recording facilities as appropriate.
- V. It is also recognised that, in the interest of security and operator safety, CCTV System owners do not wish the precise location of the relevant monitoring room to be included within the text of a Code of Practice.

3.0 FUNDAMENTAL PRINCIPLES AND POLICIES

Public Concern

Although the majority of the public at large may have become accustomed to 'being watched', those who do express concern do so mainly over matters pertaining to the processing of the information, (or data) i.e. what happens to the material that is obtained.

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

All personal data obtained by virtue of The System, shall be processed fairly and lawfully and, in particular, shall only be processed in the exercise of achieving the stated objectives of the system. In processing personal data there will be total respect for everyone's right to respect for his or her private and family life and their home.

The storage and security of the data will be strictly in accordance with the requirements of the Data Protection Act 1998 and additional locally agreed procedures.

Data Protection and Human rights Legislation

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

The 'data controller' for The System' is Rhondda-Cynon-Taf CBC and day to day responsibility for the data will be devolved to the CCTV Senior Officer.

All data will be processed in accordance with the principles of the Data Protection Act, 1998 which, in summarised form, includes, but is not limited to:

- i) All personal data will be obtained and processed fairly and lawfully.
- ii) Personal data will be held only for the purposes specified.
- iii) Personal data will be used only for the purposes, and disclosed only to the people, shown within these codes of practice.
- iv) Only personal data will be held which are adequate, relevant and not excessive in relation to the purpose for which the data are held.
- v) Steps will be taken to ensure that personal data are accurate and where necessary, kept up to date.
- vi) Personal data will be held for no longer than is necessary.
- vii) Individuals will be allowed access to information held about them and, where appropriate, permitted to correct or erase it.
- viii) Procedures will be implemented to put in place security measures to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of, information.

Human Rights Act 1998

The system will be operated by or on behalf of a public authority, the authority has considered the wider human rights issues and in particular the implications of the European Convention on Human Rights, Article 8 (the right to respect for private and family life).

Everyone has the right to respect for his private and family life, his home and his correspondence.

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.

Therefore, to comply with Article 8 (1), and Article 8 (2) RCT Council CCTV service will always considers the following:

Criminal Procedures and Investigations Act 1996

The Criminal Procedures and Investigations Act 1996 came into effect in April 1997 and introduced a statutory framework for the disclosure to defendants of material which the prosecution would not intend to use in the prosecution of its own case (known as unused material) but disclosure of unused material under the provisions of this Act should not be confused with the obligations placed on the data controller by Section 7 of the Data Protection Act 1998, (known as subject access).

Request for information (subject access)

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 system manager (CCTV Senior Officer).

The principles of Sections 7 and 8, 10 and 12 of the Data Protection Act 1998 (Rights of Data Subjects and Others) shall be followed in respect of every request

If the request cannot be complied with without identifying another individual, permission from all parties must be considered (in the context of the degree of privacy they could reasonably anticipate from being in that location at that time) in accordance with the requirements of the legislation.

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

Note Each and every application will be assessed on its own merits and general 'blanket exemptions' will not be applied.

Freedom of Information Act 2000

If a request for images is received via a FOIA application and the person requesting is the subject, these will be exempt from the FOIA and will be dealt with under The Data Protection Principles.

Any other requests not involving identification of individuals can be disclosed but only if it does not breach the data protection principles.

Regulation of Investigatory Powers Act 2000

Introduction

The Regulation of Investigatory Powers Act 2000 came into force on 2nd October 2000. It places a requirement on public authorities listed in Schedule 1: Part 1 of the act to authorise certain types of covert surveillance during planned investigations.

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 a 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: Part1 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 1984.

The Act is divided into five parts. Part II is the relevant part of the act for CCTV. It creates a system of authorisations for various types of covert surveillance. The types of activity covered

are "intrusive surveillance" and "directed surveillance". Both types of surveillance if part of a pre-planned operation will require authorisation from specified persons named in the Act. In addition, the reasons for such surveillance must be clearly indicated and fall within the criteria outlined by this legislation. A procedure is in place for regular reviews to be undertaken into authorisation.

All RCT schemes will observe the criteria laid out in the legislative requirements.

Further information is available from the Home Office website:-

www.homeoffice.gov.uk/ripa/ripact.htm

Surveillance Camera Code of Practice

The Code of Practice was a requirement of the Protection of Freedoms Act 2012 and sets out guidelines for CCTV and Automatic Number Plate Recognition (ANPR) systems to ensure their use is open and proportionate and that they are able to capture quality images that give police a better chance to catch criminals and cut crime.

The code has been built upon 12 guiding principles, which provide a framework of good practice that includes existing legal obligations. Those existing obligations include the processing of personal data under the Data Protection Act 1998, a public authority's duty to adhere to the Human Rights Act 1998 and safeguards under the Regulation of Investigatory Powers Act 2000 associated with the use of directed and covert surveillance by a public authority. The use of a surveillance camera system must:

1. Always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need
2. Take into account its effect on individuals and their privacy
3. Have as much transparency as possible, including a published contact point for access to information and complaints
4. Have clear responsibility and accountability for all surveillance activities including images and information collected, held and used
5. Have clear rules, policies and procedures in place and these must be communicated to all who need to comply with them
6. Have no more images and information stored than that which is strictly required
7. Restrict access to retained images and information with clear rules on who can gain access
8. Consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards
9. Be subject to appropriate security measures to safeguard against unauthorised access and use

10. Have effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with
11. 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, when used in pursuit of a legitimate aim
12. Be accurate and kept up to date when any information is used to support a surveillance camera system which compares against a reference database for matching purposes.

Whilst the above principles are voluntary, Local Authorities must have regard to them and RCT Council will work to achieve continued compliance with the requirements.

Information and a copy of the Codes can be found on www.gov.uk/government/uploads

4.0 Accountability and Public Information

The Public

For reasons of security and confidentiality, access to the CCTV monitoring room is restricted in accordance with this Code of Practice. However, in the interest of openness and accountability, anyone wishing to visit the room may be permitted to do so, subject to the approval of, and after making prior arrangements with, the manager of the System.

Cameras will not be used to look into private residential property. Where the equipment permits it 'Privacy zones' will be programmed into 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 the cameras. If such 'zones' cannot be programmed the operators will be specifically trained in privacy issues.

A member of the public wishing to register a complaint with regard to any aspect of The System may do so by contacting the System Manager's office. All complaints shall be dealt with in accordance with the Authority's complaints procedure. Any performance issues identified will be considered under the organisations disciplinary procedures to which all members of the Authority, including CCTV personnel are subject.

System Manager

The nominated manager named at Appendix A will have day-to-day responsibility for the system as a whole.

The system will be subject to annual audit,

The system manager will ensure that every complaint is acknowledged in writing within five working days which will include advice to the complainant of the enquiry procedure to be undertaken. A formal report will be forwarded to the nominee of the system owner named at Appendix A giving details of all complaints and the outcome of relevant enquiries.

Note: *An informal foreshortened process whereby the System Manager informs the system owners of any complaint within 7 working days would be considered Best Practice.*

Statistical and other relevant information, including any complaints made, will be included in the Annual Reports of the Authority, which are made publicly available.

Public Information

Code of Practice

A copy of this Code of Practice shall be published on the Authority's web site, and a copy will be made available to anyone on request. Additional copies will be lodged at police stations and the Authority's reception offices.

Annual Report

The annual report and that for subsequent years shall be published by the end of each financial year. A copy of the annual report will also be made available on the Authority’s web site.

Signs

Signs (As Shown below) will be placed in the locality of the cameras and at main entrance points to the relevant areas, e.g. Railway and Bus stations. The signs will indicate:

- i) The presence of CCTV monitoring;
- ii) The 'ownership' of the system;
- iii) Contact telephone number of the 'data controller' of the system.

Appendix B

5.0 Assessment of the system and Code of Practice

Evaluation

The System will periodically be independently evaluated to establish whether the purposes of the system are being complied with and whether objectives are being achieved. The format of the evaluation shall comply with that laid down by the Home Office Statistics and Research Directorate in the Home Office Bidding Guidelines and be based on assessment of The Inputs, The Outputs, The Process and the Impact of the scheme.

- i) An assessment of the impact upon crime: This assessment shall include not only the immediate area covered by the cameras but the wider town area, the Police Divisional and regional areas and national trends.*
- ii) An assessment of the incidents monitored by the system*
- iii) An assessment of the impact on town centre business*
- iv) An assessment of neighbouring areas without CCTV*
- v) The views and opinions of the public*
- vi) The operation of the Code of Practice*
- vii) Whether the purposes for which the system was established are still relevant*
- viii) Cost effectiveness*

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

It is intended that evaluations should take place at least every two years.

Monitoring

The system manager will accept day to day responsibility for the monitoring, operation and evaluation of the system and the implementation of this Code of Practice.

The system manager shall also be responsible for maintaining full management information as to the incidents dealt with by the monitoring room, for use in the management of the system and in future evaluations

Audit

The Authority’s auditor or other appropriate person, or his/her nominated deputy, who is not the system manager, will be responsible for regularly auditing the operation of the system and the compliance with this Code of Practice. Audits, which may be in the form of irregular spot checks, will include examination of the monitoring room records, digital footage history and the content of recorded material.

Inspection

A body of individuals who have no direct contact or relationship with the operation of the system may be appointed to be responsible for inspecting the operation of the system.

Inspections should take place at least once per calendar year by no more than two people at any one time. The inspectors will be permitted access to the CCTV monitoring room, without prior notice and to the records held therein at any time, provided their presence does not disrupt the operational functioning of the room. Their findings will be reported to the Auditor and their visit recorded in the CCTV monitoring room.

6.0 Control and Operation of Cameras

Guiding Principles

Any person operating the cameras will act with utmost probity at all times. All equipment used for monitoring, recording and reviewing shall at all times only be operated by persons who have been trained in their use and the legislative implications of their use.

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

Cameras will not be used to look into private residential property. 'Privacy zones' may be programmed into the system (whenever practically possible) in order to ensure that the interior of any private residential property within range of the system is not surveyed by the cameras.

Note: It may help in allaying any fears of residents living within sight of a camera for provision to be made for them to visit the monitoring room. This could provide reassurance and reinforce the professional approach adapted to the management of the system and adherence to procedures.

Camera operators will be mindful of exercising prejudices which may lead to complaints of the system being used for purposes other than those for which it is intended. The operators may be required to justify their interest in, or recording of, any particular individual, group of individuals or property at any time by virtue of the audit of the system or by the system manager.

Primary Control

Only those trained (licensed) and authorised members of staff with responsibility for using the CCTV equipment will have access to the operating controls, those operators have primacy of control at all times.

Secondary Control

Secondary monitoring facilities are provided at an alternate Location.

Subject to permission being granted by the System Manager, secondary control rooms may take control of the operation of the cameras. The use of secondary control and monitoring facilities will be administered and recorded in full accordance with this Code of Practice and the Procedural Manual and does not diminish in any way the obligations imposed on any of the persons involved to comply with all current legislative requirements

Recordings and information gathered from a 'public area' CCTV Surveillance system will be stored accordingly within specified secure storage areas.

Operational Command of the System by the Police

Under rare and extreme operational circumstances the Police may make a request to command the use of The System to which this Code of Practice applies. These circumstances may be a major incident or event that has a significant impact on the prevention and detection of crime or public safety. Such use will provide the police with a broad overview of events in order to command the incident.

Such requests will be viewed separately to the use of the systems' cameras with regard to the requirement for an authority for specific types of surveillance under the Regulation of Investigatory Powers Act 2000.

Applications made as above will be considered on the written request of a police officer not below the rank of Superintendent. Any such request will only be accommodated upon the personal written permission of the most senior representative of the System owners, or designated deputy of equal standing. In the event of an urgent need, a verbal request of the senior officer in charge, and in any case an officer not below the rank of Inspector, will be necessary. This should be followed as soon as practicable within 72 hours by a Superintendents' written request.

In the event of such a request being permitted, the Monitoring Room will continue to be staffed, and equipment operated by, only those personnel who are specifically trained to do so, and who fall within the terms of this Code. They will then operate under the command of the police officer designated in the verbal / written request, taking into account their responsibilities under this code.

In very extreme circumstances a request may be made for the Police to take total control of The System in its entirety, including the staffing of the monitoring room and personal control of all associated equipment, to the exclusion of all representatives of the System owners. Any such request should be made to The System manager in the first instance, will consult personally with the most senior officer of The System owners (or designated deputy of equal standing). A request for total exclusive control must be made in writing by a police officer not below the rank of Assistant Chief Constable or person of equal standing.

Primary Control

Only those trained (licensed) and authorised members of staff with responsibility for using the CCTV equipment will have access to the operating controls, those operators have primacy of control at all times.

Secondary Control

Secondary monitoring facilities are provided at Pontypridd Police Station

Subject to permission being granted by the System Manager, secondary control rooms may take control of the operation of the cameras. The use of secondary control and monitoring facilities will be administered and recorded in full accordance with this Code of Practice and the Procedural Manual and does not diminish in any way the obligations imposed on any of the persons involved to comply with all current legislative requirements.

Maintenance of the system

To ensure compliance with the Information Commissioners 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 Procedural Manual under a maintenance agreement.

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

The maintenance 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 of the system.

It is the responsibility of the system manager to ensure appropriate records are maintained in respect of the functioning of the cameras and the response of the maintenance organisation.

7.0 Access and Security for Control Centre and associated equipment

Authorised Access

Only trained (licensed) and authorised personnel will operate any of the equipment located within the CCTV monitoring room, (or equipment associated with the CCTV System).

Public access

Public access to the monitoring and recording facility will be prohibited except for lawful, proper and sufficient reasons and only then with the personal authority of the system manager. Any such visits will be conducted and recorded in accordance with the Procedural Manual.

Authorised Visits

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

Declaration of Confidentiality

Regardless of their status, all visitors to the CCTV monitoring room, including inspectors and auditors, will be required to sign the visitor's book and details recorded electronically on the system; this will include a declaration of confidentiality.

Note: Each page of the Visitor Book includes a declaration of confidentiality as a constant reminder of their obligations. The wording is as follows:-

In being permitted entry to this area I acknowledge that the precise location of the CCTV monitoring room is and should remain confidential. I also agree not to divulge any information obtained, overheard or overseen during my visit.

This entry accompanied by your signature in the visitors log is your acceptance of these terms.

A notice is to be displayed at the entrance to the room to inform visitors that they are entering a restricted area. A typical notice is included in Appendix C

Security

Authorised personnel will normally be present at all times when the equipment is in use. If the monitoring facility is to be left unattended for any reason it will be secured. In the event of the monitoring room having to be evacuated for safety or security reasons, the provisions of the Procedural Manual will be complied with.

Visitors and Staff enter/exit the control centre via an electronic access system - authorised personnel are supplied with a fob. Visitors are granted access manually and must sign the necessary documents as stated in this section.

Note : A fixed view camera located external to the control room provides operators with a view of persons before access is granted.

8.0 Management of Recorded Material

Guiding Principles

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

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

Members of the community must have total confidence that information recorded about their ordinary every day 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, video tape, digital tape, CD, or any form of electronic processing and storage) of the images obtained from the system, they are treated strictly in accordance with this Code of Practice and the Procedural Manual 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 the purposes defined in this Code of Practice only.

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

National standard for the release of data to a third party

Every request for the release of personal data generated by this CCTV System will be channelled through the System Manager. The System Manager will ensure the principles contained within this Code of Practice are followed at all times.

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

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

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

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

Recording Policy

Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24-hour period in 12-hour time-lapse mode, through digital multiplexers onto Digital recorders. The number of images through each multiplexer will be such that the time between successive frames once played back in time lapse mode shall not exceed 2 seconds.

Images from selected cameras will be recorded in real time at the discretion of the CCTV operators or as directed by the System Manager.

CD/DVD - Provision & Quality

To ensure the quality of the disks, and that recorded information will meet the criteria outlined by current Home Office guidelines, only CD/DVD R, are to be used with the system.

Retention

Recorded footage will be retained for a period of (31 Days) [one calendar month] before being overwritten.

CD/DVD's will be always be used and stored in accordance with the Procedural Manual. At the conclusion of their life within the CCTV System they will be destroyed and the destruction certified.

Disk Register

Each Disk will have a unique tracking record maintained in accordance with the procedural manual.

Data or electronic transfer

Provision has been made to transfer data to authorised persons via egress switch.

(UK Government CPA certification)

A full audit trail of the transfer of that data is retained on the system and recorded on the main egress account.

Evidential Footage

In the event of footage being required for evidential purposes the procedures outlined in the Procedural Manual will be strictly complied with.

Appendix A Key Personnel and Responsibilities

1. System Owners - Rhondda-Cynon-Taf CBC

The System Manager is the

CCTV Senior Officer

Tel: 01443 425005

Rhondda Cynon Taf County Borough Council

CCTV Control Centre

Ty Elai Williamstown

CF401NY

Wayne.bluck@rctcbc.gov.uk

Responsibilities:

- Rhondda-Cynon-Taf CBC is the 'owner' of the system.
- The CCTV Manager will be the single point of reference on behalf of the owners.

Appendix B RCT CCTV Sign



**CAMERÂU AR WAITH
CCTV IN OPERATION**

I ddibenion atal troseddu a diogelu'r gymuned
For the purpose of Crime Prevention and Community Safety

**CYDLYNYDD Y SYSTEM
SYSTEM OPERATOR**

01443 425005

<https://www.rctcbc.gov.uk>

Appendix C Restricted Access Notice

WARNING

RESTRICTED ACCESS AREA

Everyone, regardless of status, entering this area is required to complete an entry in the Visitors Log.

Visitors are advised to note the following confidentiality clause and entry is conditional on acceptance of that clause:

Confidentiality Clause:

'In being permitted entry to this area you acknowledge that the precise location of the CCTV monitoring room is, and should remain, confidential. You agree not to divulge any information obtained, overheard

or overseen during your visit. An entry accompanied by your signature in the Visitors Log is your acceptance of these terms'.