CLOSED CIRCUIT TELEVISION SURVEILLANCE SYSTEM

CODE OF PRACTICE

Calderdale Metropolitan Borough Council
Town Hall
Halifax
HX1 1UJ

August 2022

CONTENTS

GLOSSARY

Authorised Officer of Calderdale Metropolitan Borough Council CCTV Management	Assistant Director (Neighbourhoods), Community Safety Partnership Manager, Principal Response Officer or other appropriate officer within the Council
The Council	Calderdale Metropolitan Borough Council
Scheme area	See attached plans
Copy Downloads	A download on which footage from a master download is recorded (see para 6.4.3)
Duty Controllers	CCTV Control Room staff managed by the Council's Principal Response Officer (Community Safety)
Master Copy	A download on which video footage is recorded 'live' – either in real time or time lapsed
Police DCR	Divisional Control Room.
Police Liaison Officer	Police Officer nominated by West Yorkshire Police to liaise with authorised officers of the Council's CCTV Management and Duty Controllers on matters relating to the CCTV scheme
Scheme Owners	Calderdale Metropolitan Borough Council
Scheme Partners	British Transport Police (BTP) Halifax BID Hebden Royd Town Council Together Housing Group Calderdale Care Partnership Todmorden Town Council West Yorkshire Passenger Transport Authority (Metro) West Yorkshire Police (WYP) Woolshops Shopping Centre West Yorkshire Fire & Rescue Service (WYFRS)

1. INTRODUCTION

1.1 The use of Closed Circuit television (CCTV) is a powerful tool in the fight against crime and Anti-Social Behaviour, both in its prevention and detection.

1.2 A CCTV system installed by Calderdale Metropolitan Borough Council (The Council) covers a number of the main streets in Halifax, Brighouse, Elland, Hebden Bridge, Sowerby Bridge, Todmorden, Mytholmroyd and surface car parks in the Borough. (See appendix 3 for area of coverage). Locations for future installations will be drawn up in consultation with the Police, businesses other partners. CCTV signs are located in the areas of coverage. The system is the property of the Council. Authorised management is by Officers of the Council's Community Protection Team. Calderdale MBC is legally responsible for the system. West Yorkshire Police agree to comply with the Code of Practice.

1.3 The Council is under a duty to comply with the data protection principles set out in the Data Protection Act 2018 (see Appendix 1). The Council has considered the appropriate legislation and considers that the CCTV system meets the requirements of the data protection principles and that it is empowered, under Section 163 of the Criminal Justice and Public Order Act 1994 to provide the system to promote the prevention of crime and the welfare of the victims of crime. The Council considers the system will achieve these objectives in the following ways.

a. To assist in the reduction of Crime, Anti Social Behaviour, the fear of crime and increase the confidence of the public in the Borough.

b. Facilitate the apprehension and prosecution of offenders.

c. Assist in the prevention and detection of crime and disorder committed in public areas.

d. Deal with any public safety concerns.

e. To reduce the theft of and from cars both on-streets where CCTV is located and in car parks thus encouraging greater use of these facilities.

f. To allow positive management of traffic in the Calderdale area.

g. To increase resilience to emergency and critical incidents

The system will only be used for these objectives, and for no other purposes.

In this way, the CCTV scheme is intended to contribute to the provision of a safe and comfortable environment in the Borough for the benefit of all those who live, work or visit the areas covered by CCTV.

1.4 Appendix 1 expresses the Council's legal considerations concerning CCTV, and the appropriate legislation.

1.5 Appendix 2 refers to the Council's obligations under the Regulation of Investigatory Powers Act 2000 (RIPA) The CCTV scheme is registered with the Information Commissioner.

1.6 Through CCTV, the Council and West Yorkshire Police are working together to ensure these objectives can be achieved.

1.7 The system consists of the following component parts

- CCTV Surveillance System including cameras, brackets, poles and associated equipment covering public streets and spaces and public car parks. Current camera locations are indicated on the appended plan.
- Video and Telemetry Transmission System.
- Monitoring and control equipment at the Council's dedicated CCTV Control Room, monitoring and control equipment at the Police's Divisional Control Room Dudley Hill.

- All cameras are video recorded 24 hours per day and are constantly monitored, as established in this Code of Practice.

1.8 The CCTV system is also used for the Council's Traffic Control for traffic management purposes.

1.9 The system requires dedication and commitment, to provide a comprehensive monitoring and response service.

1.10 The system is operated in a manner that is sensitive to the privacy of people living, working and visiting the area. When setting presets for camera positions, private areas may be excluded to safeguard individual privacy.

1.11 This Code of Practice, endorsed by West Yorkshire Police, has been drawn up to ensure that any concerns over the lawfulness and integrity of the system are met. The Code of Practice must be complied with at all times. It is essential that there is public confidence in the system and that the rights of individuals are being fully protected.

2. DISCLOSURES

2.1 In order to comply with The Data Protection Act 2018, there are only limited circumstances where the Council is entitled to disclose "personal data" which is recorded by the system. Disclosure in this sense would include permitting the viewing of screens in the control room, permitting the viewing or removing of downloads or photographs, or giving West Yorkshire Police or other individuals or organisations information about recorded personal data. The Council is entitled to disclose personal data in any of these ways if

a. The purposes of the disclosure are consistent with the Council's notification to the Information Commissioner, and

b. The purposes of the disclosure fall within the objectives in 1.3 b and c above (i.e. if the purpose is the prevention or detection of crime, or the apprehension or prosecution of offenders), and if the Council has confirmation from the person seeking disclosure that the failure to disclose would prejudice those purposes, and

c. The disclosure is necessary for the exercise of the Council's functions under Section 163 of the Criminal Justice and Public Order Act 1994. See Appendix 1) or

d. The disclosure is required under a special statutory power or rule of law, or if a court orders disclosure.

2.2 In addition to this, in order to comply with the Human Rights Act 1998, the Council will only be entitled to disclose personal information in any of these ways if it can show.

a. Firstly that the restriction of these rights in Article 8 (right to respect for private and family life, home and correspondence) is in accordance with the law, i.e. that the Council is entitled to disclose under the Data Protection Act 2018 in the manner set out above.

b. Secondly, that the disclosure is for one of specified reasons, e.g. for "prevention of disorder or crime" or for "the protection of the rights and freedoms of others".

c. Thirdly, that the disclosure is proportionate to its aims and objectives, and is "necessary". This means the Council will be expected to strike a fair balance between the specified reason and the individual's enjoyment of his or her rights.

d. Fourthly, that the disclosure falls within the area of discretion within which the Council may legitimately consider a restriction of these rights to be necessary. This "margin of appreciation" which will be accorded to public authorities is difficult to predict, but if the Council is able to satisfy the conditions mentioned above, it is anticipated that the courts will leave disclosure decisions to the discretion of public authorities.

3. ACCESS TO AND SECURITY OF MONITORS/CONTROL ROOM

3.1 The CCTV Control Room is housed in Council premises in Calderdale.

3.2 Control Room staff are tasked by the CCTV Manager (Principal Response Officer) who is a Council Officer.

3.3 Access to the control room is strictly controlled and will be strictly limited to Duty Controllers and authorised management from the Council Management. The room is a secure building and staff have been instructed not to allow unauthorised access or respond to requests unless the provisions of this document apply. The Control

Room should be locked at all times. If in exceptional circumstances the monitors are to be left unattended e.g. due to emergency evacuation of the building, the control room will be secured against unauthorised entry. Any unauthorised or unnecessary intrusion into the operational functions of the control room may result in a reduction of the service provided to the public and could jeopardise the integrity, confidentiality and ethics relating to the system.

3.4 Access to view monitors, whether to operate the equipment or view the images is limited to staff with that responsibility. Public access to, or the demonstration of monitors shall not be allowed except for lawful, proper and sufficient reasons, and subject to there being no disclosure of any personal data/private information.

3.5 Particular arrangements will apply to the following:

a. Police

In general the Police should not require access to the control room. Police Officers will only enter under the following circumstances; and in each case, only on business in accordance with the objectives of the system.

i. Emergencies and major incidents, in agreement with authorised officers of the Council Management.

ii. At the request of an authorised officer of the Council Management.

iii. Police Liaison Officers authorised for the purpose.

iv. For urgent viewing of downloads and for which such viewing cannot be delayed. In these circumstances the purpose of the visit should be established prior to any admittance to the Control Room.

If Police Officers arrive unexpectedly they will not normally be admitted to the Control Room, except as in para 3.5 a. i above.

The CCTV monitor at the WYP DCR, based at Dudley Hill, Bradford is contained in a secure controlled environment. The Police apply the same strict conditions as the Council in terms of access to monitoring facilities on their property, and are fully signed up to the Council's Code of Practice.

b. Other Visitors

It is important that monitoring operations are managed with a minimum of disruption. Casual visits will not be permitted. Other visits will be subject to prior arrangements with authorised officers of the Council CCTV Management.

Priority will always be given to the uninterrupted operation of the CCTV scheme.

Filming and taking photographs will not normally be permitted within the Control Room. In exceptional circumstances where filming or photography is permitted, it will be subject to there being no disclosure of any personal data/private information.

c. Contractors

All contractors' visits will be by arrangement. All contractors will be instructed to report to an authorised officer of the Council CCTV Management in the first instance. The CCTV duty controller must be satisfied of the identity and purpose of the visit before allowing entry to the Control Room. This is particularly important outside normal visitor hours and in emergency attendance.

4. CONTROL ROOM ADMINISTRATION AND PROCEDURES - GENERAL

4.1 Control Room Administration

4.1.1 There must always be at least one duty controller present within the Control Room throughout operating hours, except in exceptional circumstances when emergency evacuation of the room is necessary.

4.1.2 A visitors' book will be maintained at the Control Room. Visitors should be requested to complete the book recording details of individual, organisation and time of arrival and departure.

4.1.3 An occurrence log must be maintained throughout operations. Brief details of incidents should be shown, including time of incident together with action taken and results noted. The identity of telephone callers and responses should always be established and noted.

4.1.4 The incidents locker will be in a computerised form on the CCTV operating system.

4.1.5 A downloads register for the use and reviewing of downloads must be completed on each shift. Continuity must be maintained, especially for evidential purposes.

4.1.6 An evidence locker must be maintained to record movement of master downloads and copy downloads from the CCTV Control Room.

4.1.7 Video downloads will be viewed in accordance with the procedures outlined in Section 6. Police viewing of video downloads will be undertaken by the Police Liaison Officer, or approved police personal by prior arrangement with an authorised officer of the Council CCTV Management. In exceptional circumstances immediate viewing of downloads may be required by the Police. In these same circumstances, the reason for the request will be established, justifying access and downloads view (para 3.5 a. iv. and para 6.5.1), again in accordance with the objectives of the system. A record will be maintained in the visitor book of all visits to view downloads.

4.1.8 A log of Request Forms and Subject Access requests will be completed.

4.1.9 Other duties may be designated to duty controllers, including liaison with other emergency services and other security systems in the Council areas as referred to in para 4.2.2 below.

4.1.10 Other administration functions will include maintaining video downloads/filing and maintaining occurrence logs.

4.1.11 Duty Controllers will be required to provide the Police and others with statements required for evidential purposes.

4.1.12 Duty Controllers must be able to recognise a request from an individual to prevent processing likely to cause substantial and unwarranted damage to that individual.

4.2 Communications

4.2.1 Dedicated telephone links with the Police DCR are provided. These will be used to relay all information on incidents that arise, and to communicate information as the incident continues. In these circumstances, verbal confirmation as the purposes of the disclosure will be accepted.

4.2.2 The emergency procedures will be used in appropriate cases to call the Fire or Ambulance Services.

In addition, liaison with other units is necessary.

Details are available within the Control Room of points of contact with the following, and are continuously updated:

Fire & Rescue Service
Ambulance Service
Shopping Centres
Retail radio 'shopwatch' schemes
Railway Stations
British Transport Police
Bus Stations
WYPTE- Metro
Halifax Police Station
Brighouse Police Station
Todmorden Police Station
Urban Traffic Control
Car Park Management
Door Security Schemes
Other CCTV Surveillance Systems in the Council area
CCTV Strategy partners
Others as necessary

4.3 Liaison

4.3.1 Regular meetings take place between the CCTV manager (Principal Response Officer), partners and other relevant stakeholders on the current functioning and potential future use of CCTV provision.

5. MONITORING PROCEDURES

Camera Controls

5.1. At least one duty controller must be present within the control room throughout operating hours (see para 4.1.1). Camera surveillance will be maintained throughout.

5.2 The control of the system will remain with the Council.

5.3 The controls must only be operated by trained staff, those under training, and those properly authorised by officers of the Council CCTV Management.

5.4 When an incident is observed by a Duty Controller, information will be immediately relayed to the Police District Control using the dedicated telephone links. The video images will also be passed to the WADC via the video link. The responsible officer in the Police WADC will then take the necessary action to ensure the incident receives the appropriate Police response. As mentioned above, verbal confirmation as to the purposes of the disclosure will be given at this stage.

5.5 Once in direct contact with the CCTV Control Room, the West Yorkshire Police Calderdale Divisional Control Room officer can request the appropriate type of monitoring from the CCTV Duty Controller. Details and responses should be noted in the occurrence log.

5.6 Close liaison and co-operation is essential at all times. Ultimate control lies with the Council as owner of the system.

5.7 Should it be necessary for the Police to stay in contact with the Duty Controller for any length of time, contact between the Calderdale CCTV Duty Controller and the Police may continue on a different line so that the dedicated direct emergency line is available for reporting any new incidents.

6.0 VIDEO DOWNLOADS PROCEDURES

6.1 Ownership

6.1.1 Ownership of recorded material remains with the Council as Data Controller. Copies may be shared with data subjects or other recipients where a lawful basis is

in place, but ownership of the contents as retained in the master downloads (see para 6.4.3) will remain with the Council. Any re-use or publication of any copy recorded material should only be after the approval of the Council has been obtained.

6.2 Recording

6.2.1 The control system is supported by video download recording facilities, which will function throughout the operations.

6.3 General Download Procedures and Use

6.3.1 Downloads recorded as per para 6.2.1 above are called master downloads.

6.3.2 The master downloads will be retained in the CCTV control room unless it is specifically required by the Police for evidence in court, or by Court Order (see section 6.4) or for image enhancement purposes.

6.3.3 An authorised officer of the Council CCTV Management will maintain a detailed downloads tracking log in the downloads register (see para 4.1.5)

6.3.4 A download will be given a unique reference number which will be marked upon it and remain with it until it is taken out of the system and destroyed.

6.3.5 Downloads will not be sold, released or used for commercial purposes or the provision of entertainment.

6.3.6 Video footage from downloads may be provided for inclusion in television programmes, only,

i) Where the purpose of that programme and the use of the CCTV footage is to assist in the identification and apprehension of offenders in relation to crime and disorder and the Police confirm that this assistance is appropriate, or,

ii) For specific educational/serious documentary purposes beneficial to the objectives of the CCTV scheme (see para 1.3) in which case all images of individuals will be obscured or disguised to protect the rights of those individuals and to prevent the disclosure of personal data/private information. Procedures and safeguards are described in para 6.4.3d.

6.3.7 Video footage / downloads of incidents will not be published or transmitted without the permission of an officer authorised by the Council CCTV Management and the appropriate Divisional Officer, West Yorkshire Police.

6.3.8 Downloads will only be released by the Council for intelligence gathering purposes, (see Section 2) if a justification can be supplied by the Police relating the need for the downloads to an ongoing criminal investigation, or investigation of known criminal offenders and where the downloads can be deemed to be useable evidence. Requests for downloads will be made by the Police Liaison Officer, or

approved police personnel. Downloads will not be released for speculative, non-specific or random intelligence gathering.

6.4 Control and Distribution of Downloads

6.4.1 It is essential that procedures for use and retention of downloads are strictly followed, for reasons of integrity, confidentiality and ethics and in order to preserve the facility to use them in future proceedings (See section 2).

6.4.2 Master Downloads

Master copy is the first down loaded footage from the CCTV system evidence locker as is normally in data format.

The following procedures must be followed -

a. The CCTV Police Liaison Officer/s must register the date and time of downloads insert, including unique downloads reference in the downloads system (see para 4.1.5)

b. Completed downloads must be stored securely by the CCTV Police Liaison Officer/s.

c. A monthly audit will be conducted by an authorised officer of CCTV Management, to ensure that the location of all downloads, match with the downloads register and evidence tracking system

d A master download will only be allowed to leave the CCTV Control Room if it contains evidence relevant to an investigation/prosecution and is required by the Police or by Court Order. The master download or sealed and signed master downloads will otherwise be securely stored in the CCTV Control Room.

e. Master downloads taken into Police possession will be identified and recorded on the Police Niche System and stored within a secure cabinet in the Connected Property Store at the relevant Police Station where it becomes the responsibility of the Police.

f. In the event of the Police requesting a large number of master downloads relating to particular incidents as part of a major incident inquiry, the Police may be asked to obtain the permission of the Council's CCTV Manager for the release of the downloads. As with individual download requests, to ensure that the rights of individuals are preserved and the chain of evidence remains intact, the Council will need to ensure that the reason(s) for which it may disclose copies of the image are compatible with the reason(s) or purpose(s) for which the images were originally obtained (see para 1.3). A specific reason or purpose must be given in the request for the requirement

for release of each download so as to balance access/disclosure with the rights of individuals, (see section 2).

h. At the conclusion of a prosecution and after the appeal period has expired (currently 28 days) the master downloads may be retained by the Police in the Connected Property Store until the end of a custodial sentence or, in the case of non-custodial sentences, for six months following the sentence. It will then be returned to the CCTV Control Room and an authorised officer of the Council will issue a receipt. In the event of an undetected crime the police may retain the master downloads for three years or longer in the case of a serious incident/s.

6.4.3 Copy Downloads

A working copy is any copy of an incident in any format which is not termed the master copy. This copy will normally be made in a DVD format from the CCTV evidence locker but can be produced from the master copy at times. Still images may be also taken in the same manner.

a. Copy downloads will normally made from the evidence locker and release of copy downloads is subject to section 2 above. Further copies may be produced by the police also subject to section 2 above.

b. West Yorkshire Police will provide a supply of blank CD's/DVD's to be used for copy downloads for the Police. Blank CD's/DVD's must be provided at no cost to the Council, by others wishing to make a copy download.

c. Where a copy download is requested by a television or other media company in accordance with para 6.3.6, the company must submit a fully justified request, in writing, to the Council, outlining the nature, scope, context, content and purpose of the programme, together with the proposed time and channel of transmission. The Council in conjunction with the Police will consider the request, following procedures outlined in para 6.3.7.

d. Downloads will only be released on the condition that the television company receive, understand and agree, in writing, to adhere to this Code of Practice, mask the identity or image of individuals subject of the video footage, and return the downloads to the CCTV Management for erasing (para 6.4.3 g). The Council and the West Yorkshire Police also retain the right to view a programme using CCTV footage prior to transmission, and reserve the right to withdraw their permission to publish if safeguards required in the Code of Practice are not complied with. The Council reserves the right to refer any concern, or dispute to the Broadcasting Complaints Commission.

e. Additional copies may be made to assist the investigating prosecution process, or the defence as referred to in section 6.5 below. Again blank CD's/DVD's must be provided at no cost to the Council, by those wishing to make the copy downloads.

6.5 Access to CCTV Control Room to View Downloads

6.5.1 Under the Data Protection Principles contained within the Data Protection Act 2018, access to images by third parties may be granted subject to the requirements of section 2 above, in limited and prescribed circumstances to the following:

a. Law enforcement agencies where the images recorded would assist in a specific enquiry.

b. Prosecution agencies

c. Relevant Legal representatives

d. The media, where it is assessed by the Council and the Police that the public's assistance is needed in order to assist in the identification of victims, witnesses or perpetrators in relation to a criminal incident (see also paras 6.3.5 - 6.3.7 and 6.4.3d). As part of that assessment, the wishes of the victim of an incident should be taken into account.

e. The people whose images have been recorded and retained (unless disclosure to an individual would prejudice the criminal enquiries or criminal proceedings). For safety and security reasons, this category of person, ("Subject Access"), will not be permitted to view downloads in the CCTV Control room. Separate arrangements elsewhere will be made (see para 6.6 below).

In cases a – c above, a CCTV Request Form will need to be submitted to the CCTV Control Room, giving reasons why the access to view downloads is requested. For “Subject Access” requests, see para 6.6 below.

Police

6.5.2 The main source of requests to view downloads is likely to be from the Police and these will be subject to the requirements of section 2 above. The method of requests will arise in a number of ways including:

i. Regular/daily requests for viewing recordings to trace incidents that have been reported, (this may be carried out through a Police Liaison Officer)

ii. Immediate action relative to live incidents, e.g. immediate pursuit

iii. Major incidents

iv. In exceptional circumstances individual Police Officers seeking to urgently view downloads and which cannot be delayed should seek written authorisation in accordance with para 3.5.a.iv from the Police Duty Inspector and be authorised by an authorised officer of the Council CCTV Management.

Other Bodies with Prosecution Powers

6.5.3 Other bodies with prosecution powers, such as the British Transport Police, Customs and Excise, the Health and Safety Executive, or Calderdale MBC Council itself, may also make requests. Again these will be dealt with in accordance with section 2 above.

. Individual and Third Party Access to downloads ("Subject access" see para 6.6 below)

6.5.4 Access to download/s may be requested in connection with civil disputes by individuals or their legal representatives in connection with criminal or civil proceedings. Again these will be dealt with in accordance with section 2 above. Where the master download is already in possession of the Police or other body with prosecution powers for evidential purposes (see para 6.5.1 - 6.5.3) then access to that evidence must be secured through the Police, or relevant prosecution body. In these latter circumstances, a copy download may be held by the CPS and the lawyer will need to sign an undertaking from the CPS in advance of receiving the copy download, to ensure its confidentiality and site storage.

6.5.5 In cases where access to download/s are requested for viewing or recording, and this accords with section 2 above, the following procedure will be followed.

i. The request must be made in writing in advance to an authorised officer of the Council's Information Management Team either through Council's Contact centre or email information.management@calderdale.gov.uk identifying as specifically as possible the time and location of the relevant incident. It will not be possible to consider vague requests.

ii. If the lawyer requires a copy download, the procedures in para 6.4.3 will be followed. In particular, attention is drawn to para 6.4.3c requiring the lawyer to make a signed undertaking to adhere to this Code of Practice.

6.5.6 The sealed master downloads will be retained in the CCTV Control Room.

d. Calderdale Council

6.5.7 Requests (see Appendix 4) must be made in writing with full justification for each and every request and be subject to approval of an authorised officer of CCTV

Management, and subject to the Council complying with the Data Protection Act 2018 and the Human Rights Act 1998.

e. Other

6.5.9 No other access to view downloads in the control room will be allowed. However, for subject access requests see section 6.6 below.

6.5.10 In all cases the viewing of downloads and the use of CD's/DVD's must be carried out with the agreement of the authorised officers of CCTV Management.

6.5.11 As stated in para 6.3.5 downloads will not be sold, released or used for commercial purposes or the provision of entertainment. Copyright of copy downloads is vested in the Council as though it was the master download.

6.5.12 The manager or other authorised council officer may disclose images to any other person or body provided that such a disclosure complies with 1.3 a to f

6.6 Subject Access Requests

6.6.1 When individuals make subject access requests (see Appendix 4), personal data will not be disclosed to that individual, if the Police or other relevant enforcement agency confirm that this would be likely to prejudice the prevention or detection of crime or the apprehension of prosecution of offenders.

Alternatively, it is possible that individuals may claim that they are entitled to access on the basis of the rights in Article 8. Any claim of this nature should be referred for advice to the Legal Services Department.

6.6.2 Under the Data Protection Act 2018, access to images by the data subject will be granted to the people whose images have been recorded and retained, unless disclosure to an individual would prejudice criminal enquiries or criminal proceedings. The following procedures apply:-

a. An individual, or their representative, may submit a request for a copy of their personal data either verbally or in writing, including via social media. As soon as practicable that request should be passed to the Council's Information Management Team. The individual must submit details of the date, time and location of the incident to allow the images to be easily found. Vague requests involving long search times may not be accepted. The individual will also be requested to submit photo identification (e.g. driving License) and any other identifying information (e.g. vehicle registration) to enable recognition.

b. When individual "subject access" requests are received, the Council CCTV Management will seek a view from the Police as to whether disclosure of the image would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. "Subject access" to view the download will only be granted if disclosure is not deemed to prejudice the above.

c. If all criteria are satisfactorily met, the Council CCTV Management will search for any images, and advise the individual by letter/email of the images which can be seen. The written response will be made within 30 days of receiving the individual's request.

d. If the identification of other individuals is inevitable through viewing the download/s, the access to view would not normally be granted without the consent of those individuals.

e. If the individual subsequently requests a copy of the relevant download extract a copy will be provided, subject to the foregoing and following criteria being met.

f. The Council CCTV Management will also need to consider whether the consent of other third parties may be required for release of the download. If unable to gain consent of 3rd parties, consideration will be given to providing 'still' images of footage to ensure confidentiality of those not the subject of the request.

g. The copy downloads will be made in the CCTV Control Room. Copyright remains with the Council.

h. It should be noted that any initial request regarding capture of (a) above must be made in full within 31 days of the incident, otherwise images will be erased in accordance with the Code of Practice.

i. All Duty Controllers must be aware of the authorised officers of the Council CCTV Management responsible for responding to the requests.

7.0 **SPECIAL CONTINGENCIES**

7.1 When major incidents arise, serious public disorder, bomb explosions/threats, serious fires, the Police may be given the authority by the Council to supervise the CCTV Control Room (see section 5). If the Police are given authority to assume control the CCTV Duty Controllers will then respond accordingly and ensure that appropriate assistance and guidance is given but will retain the operation of the equipment controls. The log should record the time at which Police assumed responsibility.

7.2 In extreme cases, if Police require sole occupation of the control room, this will be subject to agreement between the appropriate Police Chief Superintendent, and an authorised officer of the Council CCTV Management.

7.3 Emergency Evacuation Area Procedures

7.3.1 On the occasion of the Control Room lying within an emergency evacuation area, CCTV Duty Controllers will be expected to vacate the Control Room. The following procedures will be followed:

a. Cameras will be focused on the optimum positions to assist management of the incident e.g. on a possible bomb location.

b. On departure from the CCTV Control Room, the Control Room will be secured against unauthorised entry.

8.0 TRAINING

8.1 Controllers will ensure that new staff are fully briefed and trained on all functions, operational and administrative, arising within the CCTV central operation. The Police will give assistance in the training of staff, including anti-discriminatory practices.

8.2 Arrangements will also be made for staff to visit the Police's WADC. Reciprocal arrangements will be made for Police staff to visit the CCTV Control Room to view arrangements.

8.3 All staff will be given appropriate formal training to a level determined within the Council's CCTV Strategy.

9.0 COMPLAINTS

9.1 Complaints about the system to be made to the authorised officers of Calderdale MBC Town Hall Halifax HX1 1UJ. All complaints will be dealt with in the same way as the Council's Complaints Procedure. Authorised officers of Community Services Management will record all complaints about the system.

10.0 OTHER

10.1 Breaches of this Codes of Practice by staff may lead to disciplinary action being taken that could result in dismissal and staff may be subject to possible criminal proceedings.

10.2 Downloads will only be used for internal disciplinary action where the Council is permitted to do so under the Data Protection Act, and the Human Rights Act 1998.

APPENDIX 1

The Data Protection Act 2018 and Data Protection Principles

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government.

Everyone responsible for using personal data has to follow strict rules called 'data protection principles. They must make sure the information is:

- Used fairly, lawfully and transparently
- Used for specified, explicit purposes
- Used in a way that is adequate, relevant, and limited to only what is necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- Race
- Ethnic background
- Political opinions
- Religious beliefs
- Trade union membership
- Genetics
- Biometrics (where used for identification)
- Health
- Sex life or orientation
- There are separate safeguards for personal data relating to criminal convictions and offences.

Your rights

Under the Data Protection Act 2018, you have the right to find out what information the government and other organisations store about you. These include the right to:

- Be informed about how your data is being used
- Access personal data
- Have incorrect data updated
- Have data erased
- Stop or restrict the processing of your data
- Data portability (allowing you to get and reuse your data for different services)
- Object to how your data is processed in certain circumstances

You also have rights when an organisation is using your personal data for:

automated decision-making processes (without human involvement)
profiling, for example to predict your behaviour or interests

1. Calderdale MBC is under a duty to comply with the data protection principles set out in the Data Protection Act 2018.

2.1 The first of those principles requires personal data to be processed "fairly, lawfully and transparently" and prohibits the processing of personal data unless certain conditions are met.

2.2 Where personal data are processed for the prevention or detection of crime or the apprehension or prosecution of offenders, there is an exemption from this first principle to the extent to which it can be said that the application of that principle "would be likely to prejudice" the prevention or detection of crime or the apprehension or prosecution of offenders.

2.3 It is clear that the processing of personal data by the Council in this way is lawful. Section 163 of the Criminal Justice and Public Order Act 1994 empowers a local authority to provide apparatus for recording visual images of events occurring on any land in their area if it considers this will promote the prevention of crime or the welfare of the victims of crime. (The common law duty of confidentiality, and the potential implications of the Human Rights Act 1998 are referred to below). The Council considers the system will achieve these objectives in the following ways

a. By reducing the fear of crime and offering reassurance to the public

b. By assisting in the prevention of crime committed in public areas and

c. By facilitating the apprehension and prosecution of offenders

d. By assisting in traffic management

The system will only be used for these objectives, and for no other purposes.

2.4 In order for processing to be "fair" the first principle generally requires certain information about the identity of the data controller and the purposes for which data are intended to be processed to be provided to or made readily available to the data subject "so far as practicable". The draft guidance from the Data Protection Office suggests (although this is not a requirement of the Act) that this should be done at the point of obtaining the images of data subjects, and makes certain recommendations about the size and content of signs. Paragraphs (1.2) of this Code incorporates those recommendations.

2.5 As a result, the Council is of the view that the system does result in the fair and lawful processing of personal data. However, if it could be said, for any other reason, that the processing of personal data by the system is not "fair" the Council considers the system is entitled to the exemption from this principle on the basis that any additional requirement of fairness would prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders.

2.6 The conditions referred to in the first principle, and mentioned above must of course still be met. In the case of personal data in the system which is not sensitive personal data, the Council considers that the system satisfies at least one of the conditions in Schedule 2 of the 2018 Act in that the processing is necessary for the exercise of its functions under the 1994 Act. Alternatively, the Council takes the view that the processing is necessary for the purposes of its legitimate interests, and that the processing is not unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of data subjects.

2.7 It is in the nature of the system that there will be processed data which is sensitive personal data under the 2018 Act, in that there will be information as to the commission of alleged commission of offences by data subjects. The Council considers that at least one of the conditions in Schedule 3 of the 2018 Act is also met, in that again, the processing is necessary for the exercise of its functions under the 1994 Act.

3.1 The second data protection principle requires personal data be used for specified, explicit purposes and shall not be further processed in any manner incompatible with those purposes. Purposes may be specified in a notification given to the Data Protection Commissioner under the 2018 Act, and this notification will be given by the Council specifying the purposes identified in 2.3 above.

3.2 The Council considers the purposes of the system to be lawful for the following reasons

a. Calderdale MBC has the necessary powers in the 2018 Act to operate the system for the purposes specified in section 2 above.

b. The Council considers it is highly unlikely that the data in the system could be said to be information having the necessary quality of confidence about it for the common law duty of confidence to arise. Similarly, it does not seem that this would be information communicated or made known to the Council in circumstances entailing an obligation of confidence. In any event, the courts have accepted that the public interest in maintaining confidence must be weighed against countervailing public interests and have always refused to uphold the right to confidence when to do so would be to cover up wrongdoing.

c. It might also be said that the Council's powers under the 2018 Act are not restricted to circumstances where the Council is the prosecuting authority, and so disclosure to the relevant prosecuting authority can be taken to be part and parcel of "providing" apparatus for these purposes.

d. The Human Rights Act 1998 provides that it is unlawful for the Council to act in a way, which is incompatible with a Convention right. The Convention rights include Article 8.1, which provides “Everyone has the right to respect for his private and family life, his home and his correspondence." Whilst the ECHR has held that "private life" must not be interpreted restrictively, and comprises the right to "establish and develop relationships with other human beings" it is arguable that CCTV images of activities in areas to which the

public have unrestricted access, do not constitute part and parcel of a person's "private life" since they have chosen to conduct those activities in public. However, the ECHR has recently compared the notion of "private life" to European laws on data protection, and so may take the view that whatever is "personal data" is also part and parcel of a person's "private life." If so, it is clear that the mere holding of the images (and so it follows, their disclosure) would amount to a breach of Article 8.1. Clearly, holding CCTV images of activities in "private" areas such as a houses, flats, gardens etc. would undoubtedly amount to a breach of these rights (However, the Council also needs to be mindful that a failure to provide a CCTV system where there is public pressure so to do, might also be argued to amount to a breach of these rights.

e. Article 8.2 provides "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."

i. In these circumstances, the restriction of these rights can be said to be "in accordance with the law," in that the scope of these restrictions and the Council's powers to operate the system are regulated by the 1994 Act and the 1998 Act.

ii. The restrictions are for the specified reasons, i.e. "the prevention of disorder or crime" and "the protection of the rights and freedoms of others"

iii. The Council takes the view that the restriction of these rights is proportionate to its aims and objectives, in that this Code of Practice and the 2018 Act regulate disclosures, and the purposes and period of time for which the images are held. All reasonable precautions are taken to avoid the filming of private areas, and signs are in place making it clear where and when public areas will be filmed. The Council takes the view that the restriction is "necessary" for the prevention of crime as part of a package of measures being brought forward under Calderdale Safer and Stronger Communities Partnership and targeted initiatives by the Police, the promotion of housing and environmental improvements. The Council also considers that a fair balance has been struck between the need to prevent crime, and the enjoyment by individuals of their rights under Article 8.1.

iv. The Council considers that its decisions to restrict these rights in this way fall within the area of discretion within which it may legitimately consider a restriction to be necessary.

The second principle also prohibits further processing in a manner incompatible with the Council's specified and lawful purposes, and so requires the Council to seek to limit the uses of information or images, which it can lawfully disclose.

4.1 The third data protection principle requires that personal data are adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. The Council considers that the system complies with this principle in that its purpose is to assist the prevention of crime committed in public areas, and accordingly this specifies that all reasonable precautions are to be taken to avoid the filming of private areas. In addition, this Code specifies quality criteria for the type and proper use of downloads so as to avoid blurred or indistinct images and so as to ensure downloads could be used in evidence in appropriate cases.

5.1 The fourth data protection principle requires that personal data shall be accurate. Again, this Code provides quality criteria for the type and proper use of downloads (including cleaning, reuse and replacement) and procedures for checking, and if necessary amending time and location references. As a result, the Council considers that the system complies with this principle.

6.1 The fifth data protection principle requires that personal data processed for any purpose shall not be kept for longer than is necessary for that purpose. The draft guidance from the Data Protection Office indicates that town centre schemes generally do not retain recorded images for more than 30 days. This Code at para 5.4.2d specifies a general period for retention, and additional periods where the Council receives a subject access request, or a request for disclosure from the police or media. As a result, the Council considers that the system complies with this principle.

7.1 The sixth data protection principle requires data is handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage. The Council considers that the system complies with this principle.

Appendix 2

Regulation of Investigatory Powers Act 2000 -Guidance

Introduction

The Regulation of Investigatory Powers Act ("The Act") came into force on2nd 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.

The guidance contained in this Code of Practice serves to explain and highlight the legislation to be considered.

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 crime "hot spots" in order to identify and arrest offenders. Trading standards or HM Customs & Excise officers might covertly observe and then visit shops 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 normally sensory perception, such as binoculars, or the use of cameras, where this does not involve **systematic surveillance of an individual**. It forms part of the everyday functions of law enforcement or other public bodies. This low-level activity will not usually be regulated under the provisions of the 2000 Act.

Neither do the provisions of the Act cover the normal, everyday use of overt CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection and to prevent crime. However, it had not been envisaged how much the Act would impact on specific, targeted use of public/private CCTV systems by 'relevant Public Authorities' covered in Schedule 1: Part 1 of the Act, when used during 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 and Criminal Evidence Act 1978.

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."

"Covert surveillance" defined

Observations that are carried out by, or with, the use of a surveillance device.

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

Part II - Surveillance types

We should clearly differentiate in this guidance between intrusive surveillance which will be great rarity for CCTV operations, and "Directed" surveillance which will be the more likely.

"Intrusive" surveillance

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

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

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

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

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

"Directed" surveillance

This level of covert surveillance is likely to be engaged more by public/private CCTV users when they are requested by "authorised bodies" to operate their cameras in a specific way; for a planned purpose or operation; where 'private information' is gained. The Act says:-
"Directed" surveillance is defined in *subsection (2) as* ***covert surveillance*** *that is undertaken in relation to* ***a specific investigation*** *or* ***a specific operation***

which is likely to result in the obtaining of ***private information*** *about a person (whether or not one specifically identified for the purposes of the investigation or operation);*

and otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an

authorisation under this Part to be sought for the carrying out of the surveillance - ***(planned).***

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

If a CCTV user is carrying out normal everyday observations by operating a particular camera to gain best information; albeit it may not be the most obvious camera to use, or the nearest to the incident being observed, that use will not be deemed to be "covert" under the terms of the act; it is using modern technology to the advantage of the operator. It will only be where CCTV cameras are to be used in a planned, targeted way to gain private information that the requirements of authorised directed surveillance need to be met.

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

Authorisations:

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

Those who can authorise covert surveillance for public authorities listed in Schedule 1: Part 1, in respect of Directed Surveillance are detailed in Article 2: Part 1 - Statutory Instrument 2417/2000: The Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) Order 2000.

E.g.:

A *Local Authority* (within the meaning of Section 1 of the Local Government Act 1999). The prescribed office as a minimum level of authority are:
Assistant Chief Officers; Heads of Service; Service Manager or equivalent.

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

The impact for staff in Police Control Rooms and CCTV monitoring centres, is that there might be a cause to monitor for some time, a person or premises using the cameras. In most cases, this will be an immediate response to events or circumstances. In this case, it would not require authorisation unless it were to continue for some time. The RIPA draft Code of Practice suggests some hours rather than minutes.

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

The 'authority' must indicate the reasons and should fall within one of the following categories:-

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

1. *In the interests of national security*

2. *For the purpose of preventing or detecting crime or preventing disorder.*

3. *In the interests of the economic well-being of the United Kingdom*

4. *In the interests of public safety*

5. *For the purpose of protecting public health*

6. *For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or*

7. *For any purpose (not falling within paragraphs (a) to (f) which is specified for the purposes of this subsection by an order made by the Secretary of State.*

Note:

Local Authorities may only utilise RIPA Authorities in respect of 2. above.

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

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

In cases where there is doubt as to whether an authorisation is required or not, it may be prudent to obtain the necessary authority verbally and then later in writing using the forms.

In any case, CCTV Operators must always seek the formal approval of the CCTV Manager, CCTV Supervisor or, in the unlikely event of either not being available, the Community Safety Manager, prior to any directed surveillance operation – other than in a response to immediate events. In the latter case, one of those named persons should be informed as soon as practicable.

Forms are available at the Calderdale CCTV Control Room and on the Council's website.

Policing examples:-

Insp. Authorisation - urgent request (up to 72hrs)

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

Supt. Authorisation - non-urgent request

Where Homicide and Major Enquiry Team (HMET) officers are acting on intelligence linked to a long term, planned operation and they wish to have a shop premises monitored from the outside over a period of days, which is suspected in dealing in stolen goods.

No authorisation required

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

Further information on the this Act and Schedules may be found on the website: **www.homeoffice.gov.uk/ripa/ripact.htm.**

Appendix 3

Location of CCTV in the Borough

Location	Number of Cameras
Halifax	22
Halifax Peoples Park	7
Brighouse	8
Sowerby Bridge	5
Todmorden	5
Hebden Bridge	6
Mytholmroyd	1
Elland	7

Mobile, deployable, and body worn cameras, if utilised, will be in accordance with 1.3 of the Code of Practice.

Appendix 4

CCTV Access Request

Information on how to apply for access to information held on the Calderdale MBC CCTV System. Subject to certain exemptions you have a right to be told whether any personal data is held about you.

You also have a right to a copy of that information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or if you agree otherwise.

An individual has the right to request closed circuit television (CCTV) footage of you. The CCTV owner (CMBC) must provide this within 1 month at no charge to the individual.

Personal request should state that the request is covered under the Data Protection Act and that the following information should be provided to clarify identification.

- Name date of birth and home address
- Specific location, time and date
- Description of yourself
- Proof of identity

Please forward your request in writing to the address below which should contain the following information or email information.management@calderdale.gov.uk

Company request name of company and person's name applying on behalf of the company with full address and telephone details.

Details of client and description

Specific location, time and date

Full details of vehicle/s involved in the request

Any other information that can assist with the review of the request

CMBC decides how they will provide the footage and can edit it/provide 'still' images to protect the identities of other people.

CMBC can refuse requests if;

- the footage has other people in it
- It would put a criminal investigation at risk

If the CCTV footage relates to a crime and the police have the footage, they will tell you if you can see it.

The CCTV Manager
Calderdale MBC
Town Hall
Halifax
HX1 1UJ

Appendix 5

Third Party Agreement

The Calderdale MBC CCTV Manager authorises approved West Yorkshire Police personal to act on his behalf and that of Calderdale MBC to ensure third party compliance with the Calderdale Closed Circuit Television Surveillance System Codes of Practice.

This is to involve the serving of the said Codes of Practise and agreement form upon any prospective third party agency **PRIOR** to the supply of working copies as referred to in 6.4.3.

The agreement form must be completed by a senior member of the authority/business for making any such request.