Kirklees Council

Code of Practice 2019
For the Operation of
Closed Circuit Television

Civic Centre 3
Market Street
Huddersfield
HD1 2TG

Contents

Appendices

Certificate of Agreement

The content of this Code of Practice is hereby approved in respect to the Kirklees Council Closed Circuit Television System and as far as is reasonably practicable, will be complied with by all who are involved in the management and operation of the system.

Signed for and on behalf of Kirklees Council

Signature: .....

Name : ..... **Position held:** .....

Dated the ..... **day of** **20**

Signed for and on behalf of Area Commander for West Yorkshire Police

Signature: .....

Name: ..... **Position held:** .....

Dated the ..... **day of** **20**

Section 1 Introduction and Objectives

1.1 Introduction

1.1.1 The Kirklees Council CCTV system has been created and is located at Civic Centre 3, Market Street Huddersfield HD1 2TG.This Code of Practice has been designed that the system is operated legally lawfully and fairly with due regard with current laws and legislation that affects the running of the system. The system comprises of a number of cameras installed at strategic locations. All of the cameras are fully operational with pan, tilt and zoom facilities and are monitored from strategic, purpose built Control Room as described above. This Code of Practice does not extend to the use and operation of cameras held by Departments for the purpose of covert surveillance. For the purposes of the Data Protection Act 2018 the 'data controller' is Kirklees Council (See Note).

1.1.2 The Kirklees Council ('Hereafter referred to as KC) CCTV system has been notified to the Information Commissioner as required by the Data Protection Act 2018. Details of key personnel, their responsibilities and contact points are shown in appendix A to this Code.

Note:. *The **data controller** is the person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are to be processed. It must be a legal entity e.g. person, organisation or corporate body and in the case of partnerships all partners may be considered to bear the responsibility.*

1.2 Partnership statement in respect of The Human Rights Act 1998

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

1.2.2 This assessment is evidenced by an agreed 'operational requirement 'document (and any survey or consultation where applicable). 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 Partnership towards their duty under the Crime and Disorder Act 1998

1.2.3 It is recognised that operation of the Kirklees CCTV System may be considered an infringement on the privacy of individuals. The partnership recognises that it is their responsibility to ensure that the scheme should always comply with all relevant legislation in order to ensure its legality and legitimacy. The scheme will only be used as a proportional response to identified problems and only in so far as it is necessary in a democratic

society, in the interests of national security, for public safety, for the economic wellbeing of the area, for the prevention and detection of crime or disorder, for the protection of health and morals or for the protection of rights and freedoms of others.

1.2.4 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 that there is absolute respect for everyone's right to a free trial.

1.2.5 The Kirklees CCTV 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 gender, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

1.3 Aims & Objectives of the System

1.3.1 The Aims of the scheme are:

a) To work in partnership towards safer neighbourhoods for the community, visitors and anyone who works in the District.

b) To enable the areas covered by overt CCTV cameras to be safe and reduce risks to the public from crime and disorder and all the Objectives below.

The areas covered by CCTV cameras include the town centres of Huddersfield, Batley, Dewsbury, Cleckheaton, Heckmondwike, Mirfield, Birstall, Holmfirth and other public spaces determined as in need of, and provided with, CCTV coverage

1.3.2 The Objectives of the Kirklees CCTV System, as determined by the Partnership which form the lawful basis for the processing of data are:-

a) To assist in providing public confidence, reassurance and reducing levels of the fear of crime

b) To facilitate the apprehension and prosecution of offenders

c) To assist in the prevention and detection of crime and disorder committed in public areas

d) To deal with any serious public safety concerns

e) To assist in the prevention and detection of behaviour adversely affecting the environment

f) To allow positive management of traffic in the Kirklees area

1.3.3 Within this broad outline, the Partnership has drawn up, and published specific key objectives (which will be reviewed annually) based on local concerns.

1.4 Procedural Manual

1.4.1 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 that the purpose and principles (see Section 2) of the CCTV system are realised, the procedural manual is based upon and expands on the contents of this Code of Practice.

Section 2 Statement of Purpose and Principles

2.1 Purpose

2.1.1 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 Kirklees CCTV System, (hereafter referred to as 'The System') and to outline how it is intended to do this.

2.1.2 The purpose of the System, and the process adopted in determining the reasons for implementing the System, are as previously defined in Section 1.

2.2 General Principles of Operation

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

2.2.2 The operation of the system will also recognise the need for formal authorisation of any covert surveillance that falls within the definition of 'Directed Surveillance' under the Regulation of Investigating Powers Act 2000 (see Appendix G).

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

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

2.2.5 The system will be operated with due regard to the principle that everyone has the right to his or her privacy and that of family life and their home.

2.2.6 The public interest in the operation of the system will be recognised by ensuring the security and integrity of operational procedures.

2.2.7 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 shown that the System is not only accountable but is seen to be accountable.

2.2.8 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.

2.3 Copyright

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

2.4 Cameras and Area Coverage

2.4.1 The Areas covered by CCTV to which this Code of Practice refers are all public areas within the responsibility of the operating partners, including the town centres of Huddersfield,Batley, Dewsbury,Cleckheaton, Heckmondwike, Mirfield, Birstall and Holmfirth.

2.4.2 From time to time transportable or mobile cameras may be temporarily sited within the Area. The use of such cameras, and the data produced by virtue of their use, will always be in accordance with the objectives of the CCTV System and be governed by these Codes and Procedures.

2.4.3 All cameras have pan tilt and zoom (PTZ) operation, and whilst most have full colour capability some may automatically switch to monochrome in extremely low light conditions.

2.4.4 None of the cameras forming part of the System will be installed in a covert manner. The presence of CCTV cameras will be identified by appropriate signs.

2.4.5 A map showing the number and location of all fixed cameras is available for inspection.

2.5 Monitoring and Recording Facilities

2.5.1 A staffed Control Room is located at Huddersfield. The CCTV equipment has the capability of recording all public space surveillance cameras connected to the Control Room simultaneously throughout every 24 hour period.

2.5.2 No equipment, other than those housed within the main CCTV control rooms, other specified council buildings or controls rooms used by Council partners shall be capable of recording images from any of the cameras.

2.5.3 CCTV operators are able to record images from selected cameras in time-lapse mode (approximately 5 frames per second), produce hard copies of 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.

2.6 Human Resources

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

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

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

2.7 Processing and Handling of Recorded Material

2.7.1 All recorded material, whether recorded digitally, in analogue format or as a hard copy video print, will be processed and handled strictly in accordance with this Code of Practice and the Procedural Manual.

2.8 Operators Instructions

2.8.1 Technical instructions on the use of equipment housed within the Control Rooms are contained in separate manuals provided by the equipment suppliers.

2.9 Changes to the Code or the Procedural Manual

2.9.1 Any major changes either to the Code of Practice or the Procedural Manual, (i.e. those that 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.

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

Section 3 Privacy and Data Protection

3.1 Public Concern

3.1.1 Although the majority of the public at large may have become accustomed to the use of CCTV cameras, 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, including;*

i) Organisation, adaptation or alteration of the information or data;
ii) Retrieval, consultation or use of the information or data;
iii) Disclosure of the information or data by transmission, dissemination or otherwise making available, or
iv) Alignment, combination, blocking, erasure or destruction of the information or data.

3.1.2 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 absolute regard for everyone's right to respect of their private life, family life and their home.

3.1.3 The storage and security of the data will be strictly in accordance with the requirements of the Data Protection Act 2018 and additional locally agreed procedures.

3.2 Data Protection Legislation

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

3.2.2. The data controller for the System is Kirklees Council and day to day responsibility for the data will be devolved to the System manager.

3.2.3 All data will be processed in accordance with the principles of the Data Protection Act, 2018 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) Personal data held will be that which is adequate, relevant and not excessive in relation to the purpose for which the data is held.

v) Steps will be taken to ensure that personal data is 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.

Section 4 Accountability and Public Information

4.1 The Public

4.1.1 For reasons of security and confidentiality, access to the CCTV Control Room is restricted in accordance with this Code of Practice. However, in the interest of openness and accountability, Partners 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.

4.1.2 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.
4.1.3 A member of the public wishing to register a complaint with regard to any aspect of the System may do so by either contacting the Control Centre Manager’s office or logging the complaint on line through the Kirklees.gov.uk website, under “complain to the Council”. All complaints shall be dealt with in accordance with Kirklees Council’s complaints procedure, a copy of which may be obtained from the Kirklees Council offices. Any performance issues identified will be considered under the organisations disciplinary procedures to which all members of Kirklees Council including CCTV personnel, are subject.

4.1.4 All CCTV staff are contractually subject to regulations governing confidentiality and discipline. An individual who suffers damage by reason of any negligent contravention of this Code of Practice may be entitled to compensation.

4.2 System Owner

4.2.1 The 24 Hour Service Access Manager, being the nominated representative of the system owners, will have unrestricted personal access to the CCTV control rooms and will be responsible for receiving regular and frequent reports from the operators of the system.

4.2.2 Formal consultation will take place between the owners and the operators of the system with regard to all aspects, including this Code of Practice and the Procedural Manual.

4.3 System Manager

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

4.3.2 The system manager will ensure that every complaint is acknowledged in writing within three 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.

4.3.3 Statistical and other relevant information, including any complaints made, will be included in the Annual Reports of Kirklees Council.

4.4 System Development

4.4.1 The Community Safety Executive Board, as a sub-group of the Local Strategic Partnership, provides an advisory role for the development of these services and the strategic fit within the Community Safety Strategy.

4.4.2 The development and physical infrastructure is advised by the Council's executive decision-making structure.

4.5 Public Information

4.5.1 Code of Practice
A copy of this Code of Practice shall be published on The Kirklees Council Web Site https://www.kirklees.gov.uk/beta/information-and-data/pdf/cctv-code-of-practice.pdf , and a copy will be made available to anyone on request.

4.5.2 Signs
Signs will be placed in the locality of the cameras. 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.
v) An Icon representing a camera

Section 5 Assessment of the System and Code of Practice

5.1 Evaluation

5.1.1 The System will periodically be independently evaluated to establish whether the purposes of the System are being complied with by the Information Commissioners Office and whether Objectives are being achieved. The format of the evaluation will comply with that laid down by the Home Office Statistics and Research Directorate in

the Home Office Bidding Guidelines and will 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.

5.1.2 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.

5.1.3 It is intended that evaluations should take place at least every two years and national benchmarking data will be compared where appropriate.

5.2 Monitoring

5.2.1 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.

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

5.3 Audit

5.3.1 The Community Safety Manager, or his/her nominee, 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 Control Room records and the content of recorded material.

5.3.2 The operational performance of the CCTV service is incorporated in the Community Safety annual service plan as an integral part of the Council's Performance Management policy.

5.3.3 Financial management of the service will be subject to inspection through Internal and External Audit and corporate accounting protocols.

Section 6 Human Resources

6.1 Staffing of the Control Room and those responsible for the operation of the system

6.1.1 The CCTV Control Room will be staffed in accordance with the Procedural Manual. Equipment associated with the System will only be operated by authorised personnel who will have been properly trained in its use and all control room procedures.

6.1.2 Every person involved in the management and operation of the System will be personally issued with a copy of both the Code of Practice and the Procedural Manual, will be required to sign a confirmation that they fully understand the obligations and adherence to these documents placed upon them and that any breach will be considered as a disciplinary offence. They will be fully conversant with the contents of both documents, which may be updated from time to time, and which they will be expected to comply with as far as is reasonably practicable at all times.

6.1.3 Arrangements are made for a police liaison officer and/or PCSO and/or Police Officer to be present in the control room at certain times, subject to locally agreed protocols. Any such person must also be conversant with this Code of Practice and associated Procedural Manual.

6.1.4 All personnel involved with the System shall receive training from time to time in respect of all legislation appropriate to their role.

6.2 Discipline

6.2.1 Every individual with any responsibility under the terms of this Code of Practice, and who has any involvement with the System to which they refer, will be subject to the employing Authority discipline code. Discipline rules will be applied to any breach of this Code of Practice, any breach of confidentiality, failure to pass a CRB Check or hold an SIA CCTV PSS licence.

6.2.2 The system manager will accept primary responsibility for ensuring that there is no breach of security and that the Code of Practice is complied with. The system manager has day to day responsibility for the management of the Control Room and for enforcing the rules. Non-compliance with this Code of Practice by any person will be considered a breach of discipline and dealt with accordingly including, if appropriate, the instigation of criminal proceedings.

6.3 Declaration of Confidentiality

6.3.1 Every individual with any responsibility under the terms of this Code of Practice, and who has any involvement with the System to which they relate, will be required to sign a declaration of confidentiality. (See example at Appendix E, see also Section 8 concerning access to the control room by others).

Section 7 Control and Operation of Cameras

7.1 Guiding Principles

7.1.1 Any person operating the cameras will act with utmost probity at all times.

7.1.2 The cameras, control equipment, recording and reviewing equipment shall at all times only be operated by persons who have been trained in their use and the legislative implications of their use.

7.1.3 Every use of the cameras will be in accordance with the Purposes and key Objectives of the System and shall be in compliance with this Code of Practice.

7.1.4 Cameras will not be used to look into private residential property. 'Privacy zones' shall 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. The only exception to this will be when the operators are acting on directions from the police or other law enforcement agencies in accordance with the law.

7.1.5 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.

7.2 Primary Control

7.2.1 Only trained and authorised members of staff responsible for using the CCTV equipment will have access to the operating controls.

7.3 Secondary Control

7.3.1 There is no secondary control of the Kirklees CCTV system

7.4 Operation of the System by the Police

7.4.1 Under extreme circumstances the Police may make a request to assume direction of the System to which this Code of Practice applies. Only requests made on the written authority of a police officer not below the rank of Superintendent will be considered. Any such request will only be accommodated on the personal written authority of the most senior representative of the System owners, or designated deputy of equal standing. Any request and approval referred to above will be accepted verbally or in writing. A verbal request or approval will be supported in writing as soon as is reasonably practicable.

7.4.2 In the event of such a request being permitted, the Control Room will continue to be staffed, and equipment only operated by, those personnel who are authorised to do so, and who fall within the terms of Sections 6 and 7 of this Code. They will then operate under the direction of the police officer designated in the written authority.

7.5 Maintenance of the system

7.5.1 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.

7.5.2 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.

7.5.3 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.

7.5.4 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.

7.5.5 The maintenance agreement will define the maximum periods of time permitted for attendance by the engineer and for rectification of the problem depending upon the severity of the event and the operational requirements of that element of the system.

7.5.6 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.

Section 8 Access to and Security of, Control Room and Associated Equipment

8.1 Authorised Access

8.1.1 Only trained and authorised personnel will operate the equipment located within the CCTV Control Room, (or equipment associated with the System).

8.2 Public access

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

8.3 Authorised Visits

8.3.1 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.

8.4 Declaration of Confidentiality

8.4.1 Regardless of their status, all visitors to the CCTV Control Room, including inspectors and auditors, will be required to sign the Access Control Log and a declaration of confidentiality.

8.5 Security

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

8.5.2 The Control Room will at all times be secured by ‘Magnetic-Locks’ controlled by access smart cards, with only authorised personal allowed access.

Section 9 Management of Recorded Material

9.1 Guiding Principles

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

9.1.2 Every digital recording obtained by using the System has the potential of containing material that can, at any point during its life span, be admitted in evidence.

9.1.3 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 privacy in relation to their personal life.

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

9.1.5 Access to and the use of recorded material will be strictly for the purposes defined in this Code of Practice only.

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

9.2 Release of data to a third party

9.2.1 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 Appendix C to this Code of Practice are followed at all times.

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

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

9.2.3 Members of the police service or other agency having a statutory authority to investigate and/or prosecute offences may, subject to compliance with Appendix C,

release details of recorded information to the media only in an effort to identify alleged offenders or potential witnesses.

9.2.4 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 Appendix C and the Procedural Manual.

9.2.5 It may be beneficial to make use of video 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.

9.3 Recording Policy

9.3.1 Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24 hour period in time- lapse mode, through digital multiplexers onto computer hard-drive. The number of images through each multiplexer (or the number of frames recorded on a digital system) will be such that the time between successive frames once played back in time lapse mode shall not exceed 2 seconds.

9.4 Evidential Discs

9.4.1 In the event of a disc 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
Kirklees Council

Responsibilities:
Kirklees Council is the 'owner' of the system. The 24 Hour Service Access Manager will be the single point of reference on behalf of the system owners with responsibility to:

i) Ensure the provision and maintenance of all equipment forming part of the Kirklees System is in accordance with contractual arrangements which the owners may from time to time enter into;
ii) Maintain close liaison with the system manager;
iii) Ensure the interests of the owners and other organisations are upheld in accordance with the terms of this Code of Practice;
iv) Agree to any proposed alterations and additions to the system, this Code of Practice and/or the Procedural Manual.

2. System Management
The system manager is responsible for the day-to-day operational management of the system.

Responsibilities*:*
The system manager has delegated authority for data control on behalf of the 'data controller'. Their role includes responsibility to:

i) Maintain day to day management of the system and staff;
ii) Accept overall responsibility for the system and for ensuring that this Code of Practice is complied with;
iii) Maintain direct liaison with the owners of the system;
iv) Maintain direct liaison with operating partners.

Appendix B Extracts from Data Protection Act 2018

Section 7

(1) Subject to the following provisions of this section and to sections 8 and 9, an individual is entitled:

(a) To be informed by any data controller as to whether personal data for which that individual is the data subject is being processed by or on behalf of that data controller.

(b) If that is the case, to be given by the data controller a description of:
  (i) The personal data of which that individual is the data subject;
  (ii) The purpose for which they are being or are to be processed;
  (iii) The recipients or classes of recipients to whom they are or may be disclosed,

(c) To have communicated to him/her in an intelligible form:
  (i) The information constituting any personal data of which that individual is the data subject;
  (ii) Any information available to the data controller as the source of those data;

(d) Where the processing by automatic means of personal data for which that individual is the data subject for the purposes of evaluating matters relating to him/her such as, for example, his/her performance at work, his/her creditworthiness, his/her reliability or his/her conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him/her, to be informed by the data controller of the logic involved in that decision-taking

(2) A data controller is not obliged to supply any information under subsection (1) unless he/she has received:

(a) A request in writing, and

(b) Except in prescribed cases, such fee (not exceeding the prescribed maximum) as he/she may require.

(3) A data controller is not obliged to comply with a request under this section unless he/she is supplied with such information as he/she may reasonably require in order to satisfy him/herself as to the identity of the person making the request and to locate the information which that person seeks.

(4) Where a data controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, he/she is not obliged to comply with the request unless:

(a) The other individual has consented to the disclosure of the information to the person making the request, or;
(b) It is reasonable in all the circumstances to comply with the request without the consent of the other individual.

(5) In subsection (4) the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request; and that subsection is not to be construed as excusing the data controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by omission of names or other identifying particulars or otherwise.

(6) In determining for the purposes of subsection (4)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard shall be had, in particular, to:
(a) Any duty of confidentiality owed to the other individual,
(b) Any steps taken by the data controller with a view to seeking the consent of the other individual,
(c) Whether the other individual is capable of giving consent, and
(d) Any express refusal of consent by the other individual.

(7) An individual making a request under this section may, in such cases as may be prescribed, specify that his/her request is limited to personal data of any prescribed description.

(8) Subject to subsection (4), a data controller shall comply with a request under this section promptly and in any event before the end of the prescribed period beginning with the relevant day.

(9) If a court is satisfied with the application of any person who has made a request under the forgoing provisions of this section that the data controller in question has failed to comply with the request in contravention of those provisions, the court may order him/her to comply with the request.

In this section:
'prescribed' means prescribed by the Secretary of State by regulations;
'the prescribed maximum' means such amount as may be prescribed;
'the prescribed period' means forty days or such other period as may be prescribed;
'the relevant day', in relation to a request under this section, means the day on which the data controller receives the request or, if later, the first day on which the data controller has both the required fee and the information referred to in subsection (3).

(10) Different amounts or periods may be prescribed under this section in relation to different cases.

Section 8

(1) The Secretary of State may by regulations provide, in such cases as may be prescribed, a request for information under any provision of subsection (1) of section 7 is to be treated as extending also to information under other provisions of that subsection.

(2) The obligation imposed by section 7(1)(c)(i) must be complied with by supplying the data subject with a copy of the information in permanent form unless:

(a) The supply of such a copy is not possible or would involve disproportionate effort, or
(b) The data subject agrees otherwise;
(c) And where any of the information referred to in section 7(1)(c)(i) is expressed in terms which are not intelligible without explanation the copy must be accompanied by an explanation of those terms.

(3) Where a data controller has previously complied with a request made under section 7 by an individual, the data controller is not obliged to comply with a subsequent identical or similar request under that section by that individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

(4) In determining for the purposes of subsection (3) whether requests under section 7 are made at reasonable intervals, regard shall be given to the nature of the data, the purpose for which the data is processed and the frequency with which the data is altered.

(5) Section 7(1)(d) is not to be regarded as requiring the provision of information as to the logic involved in decision-taking if, and to the extent that, the information constitutes a trade secret.

(6) The information to be supplied pursuant to request under section 7 must be supplied by reference to the data in question at the time when the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.

(7) For the purposes of section 7(4) and (5) another individual can be identified from the information being disclosed if he/she can be identified from that information, or from that and any other information which, in the reasonable belief of the data controller, is likely to be in, or to come into, the possession of the data subject making the request.

Note : These extracts are for initial direction and guidance only. To ensure compliance with the legislation the relevant Data Protection legislation should be referred to in its entirety

Copies of the act and the Information Commissioner's Code of Practice can be downloaded from their website
www.gov.uk/data-protection

Appendix C National Standard for the release of data to third parties

1. Introduction

Arguably CCTV is one of the most powerful tools to be developed during recent years to assist with efforts to combat crime and disorder whilst enhancing community safety. Equally, it may be regarded by some as the most potent infringement of people's liberty. If users, owners and managers of such systems are to command the respect and support of the general public, the systems must not only be used with the utmost probity at all times, but they must be used in a manner which stands up to scrutiny and is accountable to the very people they are aiming to protect.

Kirklees Council are committed to the belief that everyone has the right to respect for his or her private and family life and their home. Although the use of CCTV cameras has become widely accepted in the UK as an effective security tool, those people who do express concern tend to do so over the handling of the information (data) which the System gathers. After considerable research and consultation, the nationally recommended standard of The CCTV User Group has been adopted by the System owners.

2. General Policy

All requests for the release of data shall be processed in accordance with the Procedure Manual. All such requests shall be channelled through the data controller although day to day responsibility may be devolved to the System Manager.

3. Primary Request to View Data

a) Primary requests to view data generated by a CCTV System are likely to be made by third parties for any one or more of the following purposes:
   - i) Providing evidence in criminal investigations or proceedings
   - ii) Providing evidence in civil proceedings or tribunals but only where directly affecting the Council.
   - iii) The prevention of crime
   - iv) The investigation and detection of crime (may include identification of offenders)
   - v) Identification of witnesses

b) Third parties, which are required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:
   - i) Police
   - ii) Statutory authorities with powers to investigate and prosecute, (e.g. Customs and Excise; Trading Standards, etc.)
   - iii) Solicitors
   - iv) Plaintiffs in civil proceedings
   - v) Accused persons or defendants in criminal proceedings

vi) Other agencies, as specified in the Code of Practice according to purpose and legal status.

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

d) In circumstances outlined at note (3) below, (requests by plaintiffs, accused persons or defendants) the data controller, or nominated representative, shall:
   i) Be satisfied that there is no inconsistency with any data held by the police in connection with the same investigation.
   ii) All such enquiries are to be processed by all parties in accordance with Section 35 of the Data Protection Act 2018.

Notes

(1) The release of data to the police is not to be restricted to the civil police but could include, (for example) British Transport Police, Ministry of Defence Police, Military Police, etc.

(2) Aside from criminal investigations, data may be of evidential value in respect of civil proceedings or tribunals. In such cases a solicitor, or authorised representative of the tribunal, is required to give relevant information in writing prior to a search being granted. In the event of a search resulting in a requirement being made for the release of data, such release will only be facilitated on the instructions of a court order or subpoena. A charge may be made for this service to cover costs incurred. In all circumstances data will only be released for lawful and proper purposes.

(3) There may be occasions when an enquiry by a plaintiff, an accused person, a defendant or a defence solicitor falls outside the terms of disclosure or subject access legislation. An example could be the investigation of an alibi. Such an enquiry may not form part of a prosecution investigation. Defence enquiries could also arise in a case where there appeared to be no recorded evidence in a prosecution investigation.

(4) The data controller shall decide which (if any) "other agencies" might be permitted access to data. Having identified those ‘other agencies’, such access to data will only be permitted in compliance with this Standard.

(5) The data controller can refuse an individual request to view if insufficient or inaccurate information is provided. A search request should specify reasonable accuracy (could be specified to the nearest ½ hour).

4. Secondary Request to View Data

a) A 'secondary' request for access to data may be defined as any request being made which does not fall into the category of a primary request. Before complying with a secondary request, the data controller shall ensure that:
   i) The request does not contravene, and that compliance with the request would not breach, current relevant legislation, (e.g. Data Protection Act 2018, Human Rights Act 1998, section 163 Criminal Justice and Public Order Act 1994, etc.);
   ii) Any legislative requirements have been complied with, (e.g. the requirements of the Data Protection Act 2018);
   iii) Due regard has been taken of any known case law (current or past) which may be relevant, (e.g. R v Brentwood BC ex p. Peck) and
   iv) The request would pass a test of 'disclosure in the public interest'.

b) If, in compliance with a secondary request to view data, a decision is taken to release material to a third party, the following safeguards shall be put in place before surrendering the material:
   i) In respect of material to be released under the auspices of 'crime prevention', written agreement to the release of the material should be obtained from a police officer, not below the rank of Inspector. The officer should have personal knowledge of the circumstances of the crime/s to be prevented and an understanding of the CCTV System Code of Practice.
   ii) If the material is to be released under the auspices of 'public well being, health or safety', written agreement to the release of material should be obtained from a senior officer within the Local Authority. The officer should have personal knowledge of the potential benefit to be derived from releasing the material and an understanding of the CCTV System Code of Practice.

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

5. Individual Subject Access under Data Protection legislation

a) Under the terms of Data Protection legislation, individual access to personal data, of which that individual is the data subject, must be permitted. Providing:
   i) The request is made in writing;
   ii) The data controller is supplied with sufficient information to satisfy him or herself as to the identity of the person making the request;

iii) The person making the request provides sufficient and accurate information about the time, date and place to enable the data controller to locate the information which that person seeks, (it is recognised that a person making a request is unlikely to know the precise time. Under those circumstances it is suggested that within one hour of accuracy would be a reasonable requirement);

iv) The person making the request is only shown information relevant to that particular search and which contains personal data of her or himself only, unless all other individuals who may be identified from the same information have consented to the disclosure;

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

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

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

i) Not currently and, as far as can be reasonably ascertained, not likely to become, part of a 'live' criminal investigation;

ii) Not currently and, as far as can be reasonably ascertained, not likely to become, relevant to civil proceedings;

iii) Not the subject of a complaint or dispute which has not been actioned;

iv) The original data and that the audit trail has been maintained;

v) Not removed or copied without proper authority;

vii) For individual disclosure only (i.e. to be disclosed to a named subject)

6. Process of Disclosure:

a) Verify the accuracy of the request.

b) Replay the data to the requester only, (or responsible person acting on behalf of the person making the request).

c) The viewing should take place in a separate room and not in the control or monitoring area. Only data which is specific to the search request shall be shown.

d) It must not be possible to identify any other individual from the information being shown, (any such information will be blanked-out, either by means of electronic screening or manual editing on the monitor screen)

e) If a copy of the material is requested and there is no on-site means of editing out

7. Media disclosure

In the event of a request from the media for access to recorded material, the procedures outlined under 'secondary request to view data' shall be followed. If material is to be released the following procedures shall be adopted:

i) The release of the material must be accompanied by a signed release document that clearly states what the data will be used for and sets out the limits on its use.
ii) The release form shall state that the receiver must process the data in a manner prescribed by the data controller, e.g. specific identities/data that must not be revealed.
iii) It shall require that proof of any editing must be passed back to the data controller, either for approval or final consent, prior to its intended use by the media (protecting the position of the data controller who would be responsible for any infringement of Data Protection legislation and the System's Code of Practice).
iv) The release form shall be considered a contract and signed by both parties**.**

8. Principles

In adopting this 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:

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

WARNING

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

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 book is your acceptance of these terms'.

Appendix E Declaration of Confidentiality

Kirklees Council CCTV System

I, ……....., am retained by Kirklees Council to

perform the duty of a 24 Hour Service Access Officer. I have received a copy of the Code of Practice in respect of the operation and management of that CCTV System.

I hereby declare that:

I am fully conversant with the content of that Code of Practice and understand that all duties which I undertake in connection with the Kirklees Council CCTV System must not contravene any part of the current Code of Practice, or any future amendments of which I am made aware. If now, or in the future, I am or become unclear of any aspect of the operation of the System or the content of The Code of Practice, I undertake to seek clarification of any such uncertainties.

I understand that it is a condition of my employment that I do not disclose or divulge to any individual, firm, company, authority, agency or other organisation, any information which I may have acquired in the course of, or for the purposes of, my position in connection with the CCTV System, verbally, in writing or by any other media, now or in the future, (including such time as I may no longer be retained in connection with the CCTV System).
In appending my signature to this declaration, I agree to abide by the Code of Practice at all times. I also understand and agree to maintain confidentiality in respect of all information gained during the course of my duties, whether received verbally, in writing or any other media format - now or in the future.
I further acknowledge that I have been informed and clearly understand that the communication, either verbally or in writing, to any unauthorised person(s) of any information acquired as a result of my employment with Kirklees Council may be an offence against the Official Secrets Act of 1911, Section 2, as amended by the Official Secrets Act of 1989.

Signed: Print Name:

Witness: Position:

Dated this day of (month) 20

Appendix F Regulation of Investigatory Powers Act Guiding Principles

Advice and Guidance for Control Room Staff and Police Inspectors in respect of CCTV and the Regulation of Investigatory Powers Act 2000.

The Regulation of Investigatory Powers Act 2000, amongst other subjects, relates to surveillance by the Police and other agencies (including Local Authorities) and deals in part with the use of directed covert surveillance. Section 26 of this Act sets out what is Directed Surveillance. It defines this type of surveillance as:

Subject to subsection (6), surveillance is directed for the purposes of this Part if it is **covert** but **not intrusive** and is undertaken-

(a) For the purposes of a specific investigation or a specific operation;
(b) In such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
(c) Otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an

authorisation under this Part to be sought for the carrying out of the surveillance.

Although the Systems cameras are overt if they are used in such a way that falls within the definition of Directed Surveillance they will only be used if the necessary verbal and / or written authorities have been given.

THE Kirklees Council CCTV SYSTEM CAMERAS WILL NOT BE USED FOR PURPOSES THAT MEET THE DEFINITION OF "INTRUSIVE SURVEILLANCE" UNLESS CORRECTLY AUTHORISED.

The impact for staff in the Police control rooms and CCTV monitoring centres, is such that there might be cause to monitor for some time, a person or premises using the cameras. In most cases, this will fall into sub section **c** above, i.e. it will be an immediate response to events or circumstances. In this case, it would not require authorisation unless it were to continue for some time. The code says some hours rather than minutes. In cases where a pre-planned incident or operation wishes to make use of CCTV for such monitoring, an authority will almost certainly be required.

In the case of authorities given by the Police these are usually authorised by a Superintendent or above. However, if an authority is required immediately, an Inspector may authorise the surveillance. The forms in both cases must indicate the reason and should fall within one of the following categories:-
An authorisation is necessary on grounds falling within this subsection if it is necessary-

(a) In the interests of national security;
(b) For the purpose of preventing or detecting crime or of preventing disorder;
(c) In the interests of the economic well-being of the United Kingdom;

(d) In the interests of public safety;
(e) For the purpose of protecting public health;
(f) For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or
(g) For any purpose (not falling within paragraphs (a) to (f)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

The RIP Act also makes provision for directed surveillance to be conducted by a Local Authority. In such cases, the written authority to carry out directed surveillance using the Kirklees Council CCTV system will only be given at Director or Service Head Level.

APPENDIX G - GLOSSARY OF TERMS
Basic CCTV Terminology

Analogue Recorder: A video recorder that records by laying information onto a tape by rearranging magnetic particles, the information can be retrieved at a later date.

Angle of View: The limit of the viewing area of a camera/lens com

Audit Trail (Digital): An audit trail is a way of authenticating a digital image. It comprises a digital signature made up of a 'fingerprint' related to information about the capture of the image. Audit trails are widely used by the police in audio recordings, and an audit trail on a digital recorder can show a combination of vital details on each video frame. These can include time and date of creation and the camera on which the image was recorded to prove beyond doubt that an event happened at a particular time.

Automatic Iris: A lens which automatically adjusts its aperture to match the varying light levels to provide a constant picture.

Bandwidth: Bandwidth determines the amount of data that can be transmitted in a fixed amount of time. For digital devices the bandwidth is generally expressed in bits per second (bps) or bytes per second (Bps). For analogue systems the bandwidth is expressed in cycles per second, or Hertz (Hz).

CCD: A Charge Coupled Device. In layman's terms a silicone chip used in a camera as an imaging device. (the larger the chip the more powerful the camera)

CCTV: A closed circuit television or private system, not for general public broadcasting

CIF: Common Intermediate Format - a set of standard video formats used in digital recording, defined by their resolution.

CIF (resolution 360 x 240)
2CIF (resolution 720 x 240)
4CIF (resolution 720 x 480)

Digital Video Recorder: A method of recording information digitally initially onto a hard disk which can be retrieved or downloaded to another recording media such as tape, DVD or CD. It retains quality better than analogue recorders.

Dummy Camera: looks like a real camera but not capable of recording

DVD: Digital Versatile Disc. A data encoding standard for CD-ROM-like discs, capable of storing data at the higher densities needed for recording movies. A typical DVD contains 4.7 Gigabytes of data, and can record approximately 90 minutes of video footage

Dwell Time: The amount of time that a camera views an area before automatically moving to another position.

Fibre Optic: An efficient method of transmitting video etc. over distances using fibre optic cable. Constructed using thin fibres of glass and laser light technology and encased in armour cabling to protect the delicate fibres

Field of View: The image area transmitted by a lens.

Frame: A single camera or film image.

Frame Rate: The rate at which frames are to be output from the decoding process. E.g. real-time images are 25 frames per second

Hard Disk Drive: Electro mechanical device used to store large amounts of digital data. They are the most common storage medium used in digital video recorders.

Hard wired: A single or multi-core cable used to pass video and telemetry signals usually on short runs. E.g. coaxial or fibre optic cables

HRA 1998: An act of law introduce to uphold certain rights of the public such as article 6 a right to a fair trial and article 8 a right to a private and family life, full endorsed and adhered to by C.O.L.C.

Infra-Red: A range of frequencies just below the human visible spectrum. It is used for transmitting information or providing additional illumination for cameras. Used to enhance CCTV images where there is no artificial light e.g. Works depots or public parks.

IP camera: A type of CCTV camera that outputs video as digital information usually according to the TCP/IP protocol.

Lux: The metric unit for the measurement of light.

Microwave Transmission: A method transmitting video and telemetry signals through the air, known as line of sight transmission

Monochrome: A black and white picture comprising of a number of levels of grey scales

Motion Detection: A system for detecting movement within the view of a camera, generally using a change in the grey scale of the picture.

Multiplex: Method of transmitting or presenting for recording a number of video signals from different cameras at the same time.

Operator: The person designated to operate the surveillance system

Privacy Zone: Usually electronically programmed into the CCTV system to stop accidental intrusion with the cameras into private residential widows and others areas regarded as private

Pre-set: A function programmed into the control to allow a camera to move to a precept position following an alarm or physical activation.

PSS: Public Space Surveillance, the areas mainly in a town or city centre that is under surveillance from a CCTV system.

RAID: Redundant Array of Independent Disks. A method of insuring data integrity by utilizing multiple disks. RAID organises disks into single logical units.

Resolution: the definition of a TV picture in terms of finest detail that can be recorded and played back

RIPA: Regulation of Investigatory Powers Act 2000, a law allowing the surveillance of people in private and public places.

Sensitivity:	A figure specified in lux that denotes the camera sensitivity, the smaller the number the more sensitive the camera.
Sequential Switcher:	A switcher which will provide images from cameras in a predetermined order and remaining for the pre-set dwell time.
SIA:	The Security Industry Authority. A government department set up as a result of the Private Security Act 2001 with responsibility for the licensing of individuals working in the security industry including CCTV operators
Telemetry:	an electronic method of controlling the functions of a camera e.g. the PTZ
TFT:	Thin Film Transistors, the name given to the “flat screen” monitors used to display the CCTV images. The can be either Liquid crystal display (LCD), Light Emitting Diode (LED) or Plasma screens
Time Lapse:	A video recording that stretches the recording time by recording fewer frames per second, various time lapses are available depending on the manufacturer.
Touch Screen Control:	Also known as a Graphical User Interface, a special monitor used to display control functions of cameras etc. the touching of relative areas of the screen produces control features as in a normal system.
VCR:	Video Cassette Recorder, the machine that records images onto video tape
VHS:	Video Home System. This is the name given to tape format of domestic and small security system video recorders.
Zoom Ratio:	Where the lens has moveable elements, figures are given to show the relative magnification.